Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften – De-Mail-Gesetz

A. Problem und Ziel

E-Mails sind zu einem Massenkommunikationsmittel geworden, das privat ebenso selbstverständlich genutzt wird wie in der Kommunikation mit Behörden und Geschäftspartnern. Denn E-Mails sind einfach, schnell, preiswert und ortsunabhängig. Doch E-Mails können mit wenig Aufwand auf dem Weg abgefangen, wie Postkarten mitgelesen und in ihrem Inhalt verändert werden. Vorhandene Möglichkeiten von Verschlüsselungslösungen haben sich nicht in der Fläche durchsetzen können. Sender und Empfänger können nie sicher sein, mit wem sie gerade tatsächlich kommunizieren.

Um die Funktionsfähigkeit und Akzeptanz der elektronischen Kommunikation trotz steigender Internetkriminalität und wachsender Datenschutzprobleme zu erhalten und auszubauen, wird eine zuverlässige und geschützte Infrastruktur notwendig, die die Vorteile der E-Mail mit Sicherheit und Datenschutz verbindet. Mit den De-Mail-Diensten soll eine solche Infrastruktur eingeführt werden. Im Rahmen eines Akkreditierungsverfahrens haben De-Mail-Diensteanbieter nachzuweisen, dass die durch sie angebotenen E-Mail-, Identitätsbestätigungs- und Dokumentenablagedienste hohe Anforderungen an Sicherheit und Datenschutz erfüllen. Der Gesetzentwurf bietet den Rechtsrahmen, der die Anforderungen an die Vertrauenswürdigkeit der Diensteanbieter und der De-Mail-Dienste regelt, den Nachweis ihrer Erfüllung ermöglicht und die dauerhafte Sicherheit der De-Mail-Dienste gewährleistet.

B. Lösung

Der Gesetzentwurf schafft den Rechtsrahmen, der zur Einführung vertrauenswürdiger De-Mail-Dienste im Internet benötigt wird. De-Mail-Dienste akkreditierter Diensteanbieter bieten dem elektronischen Geschäfts- und Rechtsverkehr sichere Kommunikationslösungen, bei denen sich die Teilnehmer der Vertraulichkeit ihrer Kommunikation und der Identität ihrer Kommunikationspartner hinreichend sicher sein können. Zudem verbessert er die Möglichkeiten, die Authentizität von Willenserklärungen in elektronischen Geschäftsprozessen beweisen und Erklärungen nachweisbar zustellen zu können. De-Mail-Dienste sollen dadurch den elektronischen Rechts- und Geschäftsverkehr fördern.

Mit dem Gesetzentwurf wird ein Akkreditierungsverfahren für Diensteanbieter von De-Mail-Diensten eingeführt. Als Voraussetzung der Akkreditierung hat der Diensteanbieter die durch die Vorschriften dieses Gesetzes eingeführten Anforderungen zu erfüllen und dies auf die ebenfalls geregelte Art und Weise nachzuweisen. Zur Entlastung der zuständigen Behörde kann dies über anerkannte private Stellen erfolgen; die Akkreditierung selbst bleibt der zuständigen Behörde vorbehalten. Mit dem Entwurf werden zudem die Pflichtdienste für ein De-Mail-Angebot bestimmt und eine Aufsicht über die akkreditierten Diensteanbieter von De-Mail-Diensten eingeführt. Um künftig die Beweismöglichkeiten über den Zugang von Willenserklärungen im Sinne von § 130 des Bürgerlichen Gesetzbuches in elektronischer Form zu verbessern, wird in Artikel 1 § 5 Absatz 8 eine beweissichere Zugangsbestätigung eingeführt, die der Diensteanbieter des Empfängers elektronisch erzeugt.

Um künftig bei der elektronischen förmlichen Zustellung – etwa im Sinne des Verwaltungszustellungsgesetzes – die Beweismöglichkeiten über den Zugang zu verbessern, wird in Artikel 1 § 5 Absatz 9 eine beweissichere Abholbestätigung eingeführt. Außerdem erfolgt eine Anpassung des Verwaltungszustellungsgesetzes. Der Aufnahme von Regelungen zur Haftung des Diensteanbieters bedurfte es nicht. Insoweit gewähren die allgemeinen Haftungsvorschriften ausreichenden Rechtsschutz. Dies gilt auch für das Verhältnis zwischen akkreditiertem Diensteanbieter und Dritten, weil zentrale Vorschriften

des Gesetzes (insbesondere die §§ 3 bis 13, 16 bis 18, 22a) drittschützende Wirkung entfalten.

C. Alternativen

Keine. Insbesondere stellen die De-Mail-Dienste keine Alternative zur qualifizierten elektronischen Signatur nach Signaturgesetz dar. Die qualifizierte elektronische Signatur nach Signaturgesetz stellt insbesondere das Äquivalent zur handschriftlichen Unterschrift dar und dient damit der Erfüllung eines im Einzelfall erforderlichen Schriftformerfordernisses im Sinne von § 126a des Bürgerlichen Gesetzbuches (BGB), § 3a des Verwaltungsverfahrensgesetzes (VwVfG), § 87a der Abgabenordnung (AO) und § 36a des Ersten Buches Sozialgesetzbuch (SGB I). Mit den De-Mail-Diensten wird hingegen eine Plattform bereitgestellt, die – im Gegensatz zur herkömmlichen E-Mail-Kommunikation – eine sichere und nachvollziehbare Kommunikation schafft. Die bis dato fehlende Nachweisbarkeit der elektronischen Kommunikation wird mit De-Mail nunmehr möglich, da der Versand bzw. der Empfang von De-Mails nachgewiesen werden kann und die Identität der Kommunikationspartner gesichert ist. Ergänzend kann die qualifizierte elektronische Signatur vom Nutzer z. B. in den Fällen eingesetzt werden, wenn ein per De-Mail versendetes Dokument einem Schriftformerfordernis unterliegt und daher nach § 126a BGB, § 3a VwVfG, § 36a SGB I oder § 87a AO mit einer qualifizierten elektronischen Signatur nach Signaturgesetz versehen werden muss.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine

2. Vollzugsaufwand

Für den Betrieb der De-Mail-Dienste sind grundsätzlich private Diensteanbieter vorgesehen. Gleichwohl steht es auch Behörden oder sonstigen öffentlichen Stellen frei, im zulässigen Rahmen De-Mail-Dienste anzubieten. Verwaltungsaufwand entsteht durch die Akkreditierung der De-Mail-Diensteanbieter und die Aufsicht über diese. Diese Aufgaben sollen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wahrgenommen werden. Die diesbezüglich neu zu schaffenden Befugnisse des BSI sind mit einem entsprechenden Vollzugsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der Inanspruchnahme des Akkreditierungsverfahrens durch potentielle De-Mail-Diensteanbieter abhängig und daher nur schwer zu beziffern.

Beim BSI besteht aufgrund des De-Mail-Gesetzes ein Aufwand an ca. 8 zusätzlichen Planstellen/Stellen mit Mehrkosten in Höhe von jährlich rund 525.000 Euro. Beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) besteht ein Bedarf in Höhe von 3 zusätzlichen Planstellen/Stellen mit Mehrkosten in Höhe von jährlich rund 263.000 Euro. Dieser ergibt sich aus der für den BfDI neuen Aufgabe gem. § 18 Absatz 3, die vom an einer Akkreditierung interessierten Diensteanbieter vorzulegenden Nachweise zur Erfüllung der datenschutzrechtlichen Anforderungen zu prüfen und auf Antrag des Diensteanbieters ein Zertifikat zu erteilen. Außerdem ist der BfDI für die den Nachweisen zugrundeliegenden datenschutzrechtlichen Kriterien verantwortlich. Die zusätzlichen Stellen und der Mehraufwand beim BSI und beim BfDI sind aus dem Gesamthaushalt zu finanzieren. Eine Kompensation aus dem Einzelplan 06 ist nicht möglich. Der beim BSI und BfDI entstehende Mehraufwand bei den Sachkosten wird zum Teil durch noch festzulegende Gebühren für das jeweilige Verfahren (u. a. Akkreditierungsverfahren bzw. Zertifizierungsverfahren) gedeckt. Im Übrigen werden die Sachkosten grundsätzlich aus dem Einzelplan erwirtschaftet.

Kosten zur Anpassung von Verfahren der Verwaltung an die Nutzung von De-Mail-Diensten können nicht benannt werden. Sie treffen Bund, Länder und Kommunen gleichermaßen. Langfristig können Verwaltungskosten durch die Verbreitung und Nutzung der De-Mail-Dienste jedoch gesenkt werden und elektronische Geschäftsprozesse, deren Risiko sinkt, kostengünstiger angeboten werden. Die Verwaltung kann durch Nutzung der De-Mail-

Dienste insbesondere den Anteil der mit hohen Material- und Prozesskosten versehenen Papierpost reduzieren, wobei ein Einsparpotential pro Briefsendung von mindestens 0,25 Euro bis 0,50 Euro zugrunde gelegt werden kann. Da davon auszugehen ist, dass der Preis pro De-Mail-Nachricht deutlich unter den heute üblichen Portokosten liegen wird, lassen sich weitere erhebliche Einsparungen erzielen. Die Höhe der Einsparungen lässt sich allerdings gegenwärtig noch nicht beziffern, da sich marktgerechte Preise für De-Mail erst im Wettbewerb bilden müssen. Die Verwaltung versendet ca. 1,313 Milliarden Briefe (mit einem Gewicht von unter 50 g) pro Jahr. Unter der Annahme, dass von diesen 75 Prozent, also ca. 985 Millionen Briefsendungen, grundsätzlich per elektronischer Post versendet werden können und der weiteren Annahme, dass die Internetnutzung der Verwaltung bei 80 Prozent liegt, ergibt sich eine Anzahl von ca. 788 Millionen per elektronischer Post versendbarer Briefsendungen pro Jahr. Wenn die Verwaltung hiervon im ersten Jahr 2 Prozent, im zweiten Jahr 5 Prozent, im dritten Jahr 10 Prozent, im vierten Jahr 15 Prozent und im fünften Jahr nach Einführung der De-Mail-Dienste 20 Prozent über De-Mail-Dienste versendet, ergibt sich daraus ein über die ersten fünf Jahre nach Einführung der De-Mail-Dienste gemitteltes jährliches Einsparpotential von ca. 20 bis 40 Mio. Euro. Ab dem fünften Jahr kann von jährlichen Einsparungen von ca. 40 bis 80 Mio. Euro ausgegangen werden jeweils zuzüglich der eingesparten Portokosten.

E. Sonstige Kosten

Als ein Teil der Akkreditierungskosten entstehen für den Diensteanbieter Kosten für die Gewährleistung der Deckungsvorsorge (Annahme: etwa 100.000 Euro pro Jahr). Der größte Kostenblock (18,512 Mio. Euro jährlich) ergibt sich durch die Pflicht zur zuverlässigen Identitätsfeststellung bei der Erstregistrierung von Kunden.

Diesen Kosten steht ein Einsparpotenzial gegenüber, das sich daraus ergibt, dass Bürgerinnen und Bürger, Wirtschaft (Unternehmen) und Verwaltung durch Nutzung der De-Mail-Dienste insbesondere den Anteil der mit hohen Porto-, Material- und Prozesskosten versehenen Papierpost reduzieren können. Das Einsparpotenzial pro Briefsendung beläuft sich für Wirtschaft und Verwaltung auf 0,25 Euro bis 0,50 Euro zuzüglich der Portoeinsparungen sowie für Bürgerinnen und Bürger auf 0,08 Euro bis 0,15 Euro zuzüglich der gegenwärtig noch nicht Portoeinsparungen.

Bei einer konservativen Nutzenbetrachtung wird ferner davon ausgegangen, dass pro Jahr ca. 17,5 Milliarden Briefsendungen im lizenzpflichtigen Bereich verschickt werden. Weiterhin wird angenommen, dass davon bereits im fünften Jahr etwa 1,5 Milliarden Briefsendungen (9 Prozent) durch De-Mail-Nachrichten ersetzt werden. Diese verteilen sich zu ca. 80 Prozent auf die Wirtschaft und zu jeweils 10 Prozent auf öffentliche Verwaltung sowie Bürgerinnen und Bürger.

Falls man die zu erwartenden Portokosteneinsparungen unberücksichtigt lässt, beträgt das jährliche Einsparpotenzial im fünften Jahr ca. 363 bis 725 Mio. Euro und verteilt sich wie folgt:

Wirtschaft: 315 Mio. Euro bis 630 Mio. Euro;

Verwaltung: 39 Mio. Euro bis 79 Mio. Euro;

Bürgerinnen und Bürger: 9 Mio. Euro bis 16 Mio. Euro.

F. Bürokratiekosten

Durch das De-Mail-Gesetz werden insgesamt acht neue Informationspflichten für die Wirtschaft eingeführt. Diese beziehen sich auf die Diensteanbieter, die sich für die Erbringung von De-Mail-Diensten akkreditieren lassen. Die Verteilung ist wie folgt:

● Akkreditierung der Diensteanbieter: drei neue Informationspflichten

● Betrieb von De-Mail-Diensten: vier neue Informationspflichten

● Einstellung der Tätigkeit: eine neue Informationspflicht.

Im Rahmen des Ex-Ante-Verfahrens werden die daraus resultierenden Bürokratiekosten auf

ca. 2,5 Mio. Euro jährlich beziffert.

Die vorgesehenen Regelungen sind zwar mit Kosten für die künftigen Diensteanbieter verbunden, insgesamt wird die Wirtschaft aber erheblich entlastet, da die neuen Möglichkeiten der elektronischen Kommunikation auf Basis der De-Mail-Dienste zu großen Einsparungen bei der papierbasierten Kommunikation führen.

Für den Nutzer eines De-Mail-Kontos werden zwei neue Informationspflichten eingeführt: Der Nutzer hat zur Eröffnung eines De-Mail-Kontos einen Antrag zu stellen, bei dem Angaben zur Identitätsfeststellung gemacht werden müssen. Außerdem entsteht eine Informationspflicht im Zusammenhang mit der Freischaltung des De-Mail-Kontos.

Für die Verwaltung, d. h. für die zuständige Behörde werden vier neue Informationspflichten im Rahmen der Akkreditierung von Diensteanbietern sowie der Aufsicht eingeführt. Da von ca. 20 akkreditierten Diensteanbietern nach fünf Jahren ausgegangen wird, sind diese Bürokratiekosten im Vergleich zu den erwarteten Einsparungen für die Verwaltung gering. Die Saldierung erwarteter Mehrkosten und erwarteter Kostenreduzierungen allein durch den Einsatz von elektronischen Nachrichten anstelle von Papierpost wird zu einer deutlichen Kosteneinsparung bei der Verwaltung führen.

Bezogen auf die Bürokratiekosten der Wirtschaft aus Informationspflichten kann sich ein bedeutsames Einsparpotential allein aufgrund der zu erwartenden Portokosteneinsparungen ergeben, welches zur Zeit allerdings noch nicht beziffert werden kann.

Entwurf

eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften (De-Mail-Gesetz)[1]

vom [Datum der Ausfertigung]

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

De-Mail-Gesetz

Abschnitt 1

Allgemeine Vorschriften

§ 1

De-Mail-Dienste

(1) De-Mail-Dienste im Sinne dieses Gesetzes bilden eine elektronische Kommunikationsplattform im Internet, deren Dienste sicheren elektronischen Geschäftsverkehr für jedermann ermöglichen und das Internet als Mittel für rechtsverbindliches und vertrauliches Handeln ausbauen.

(2) De-Mail-Dienste im Sinne dieses Gesetzes ermöglichen eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post und die Nutzung eines Verzeichnisdienstes sowie optional von Identitätsbestätigungs- und Dokumentenablagediensten. Ein De-Mail-Dienst wird von einem nach diesem Gesetz akkreditierten Diensteanbieter betrieben.

§ 2

Zuständige Behörde

Zuständige Behörde nach diesem Gesetz und den Rechtsverordnungen nach § 24 ist das Bundesamt für Sicherheit in der Informationstechnik.

[1] Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.7.1998, S. 37), die zuletzt durch die Richtlinie 2006/96/EG vom 20. November 2006 (ABl. L 363 vom 20.12.2006, S. 81) geändert worden ist, sind beachtet worden.

Abschnitt 2

Pflichtangebote und optionale Angebote des Diensteanbieters

§ 3

Eröffnung eines De-Mail-Kontos

(1) Jeder kann bei einem akkreditierten Diensteanbieter einen Bereich in einem De-Mail-Dienst beantragen, welcher nur ihm zugeordnet ist und nur von ihm genutzt werden kann (De-Mail-Konto). Eine natürliche Person muss zum Zeitpunkt der Antragstellung mindestens 16 Jahre alt sein.

(2) Der akkreditierte Diensteanbieter hat die Identität des Antragstellers zuverlässig festzustellen. Dazu erhebt er folgende Angaben:

1. bei einer natürlichen Person Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift;
2. bei einer juristischen Person oder 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) Zur Überprüfung der Identität des Antragstellers hat sich der akkreditierte Diensteanbieter anhand der nachfolgenden Dokumente zu vergewissern, dass die nach Absatz 2 Satz 2 erhobenen Angaben zutreffend sind:

1. bei natürlichen Personen anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes oder anhand von Dokumenten mit gleichwertiger Sicherheit; die Überprüfung der Identität kann auch anhand des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes erfolgen.
2. bei juristischen Personen oder Personengesellschaften oder öffentlichen Stellen anhand eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in die Register- oder Verzeichnisdaten.

Der akkreditierte Diensteanbieter darf dazu mit Einwilligung des Antragstellers personenbezogene Daten verarbeiten oder nutzen, die er zu einem früheren Zeitpunkt erhoben hat, sofern diese Daten die zuverlässige Identitätsfeststellung des Antragstellers gewährleisten.

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

1. der akkreditierte Diensteanbieter den Antragsteller eindeutig identifiziert hat und die Identitätsdaten des Antragstellers erfasst und erfolgreich überprüft wurden,

2. der akkreditierte Diensteanbieter dem Antragsteller seine Anmeldedaten auf geeignetem Wege übermittelt hat und

3. der Antragsteller im Rahmen einer initialen Anmeldung nachgewiesen hat, dass er die Anmeldedaten erfolgreich nutzen konnte.

(5) Dem akkreditierten Diensteanbieter obliegt als allgemeine Sorgfaltspflicht auch nach der Eröffnung des De-Mail-Kontos eines Nutzers, dass die zu diesem Nutzer vorgehaltenen Identitätsdaten mit den vorhandenen Informationen über den Nutzer übereinstimmen. Er hat sicherzustellen, dass die jeweiligen Nachweise und Informationen in angemessenem zeitlichem Abstand auf ihre Aktualität überprüft werden.

§ 4

Sichere Anmeldung zu einem De-Mail-Konto

(1) Der akkreditierte Diensteanbieter ermöglicht dem Nutzer eine sichere Anmeldung zu dem De-Mail-Konto und damit zu den einzelnen Diensten. Der akkreditierte Diensteanbieter muss sicherstellen, dass eine sichere Anmeldung nur dann erfolgt, wenn der Nutzer ein hierfür geeignetes Verfahren einsetzt. Ein Verfahren ist geeignet, wenn es durch zwei voneinander unabhängige Sicherungsmittel gegen eine unberechtigte Nutzung geschützt ist sowie die Einmaligkeit und Geheimhaltung der im Rahmen des Verfahrens verwendeten Geheimnisse sichergestellt ist. Die Anmeldung an ein De-Mail-Konto erfolgt auf Verlangen des Nutzers nur als sichere Anmeldung. Der akkreditierte Diensteanbieter hat den Nutzer vor der erstmaligen Nutzung des De-Mail-Kontos über die Möglichkeit und über die Bedeutung einer sicheren Anmeldung zu unterrichten. § 9 Absatz 2 gilt entsprechend.

(2) Der akkreditierte Diensteanbieter hat zu gewährleisten, dass dem Nutzer mindestens zwei Verfahren zur sicheren Anmeldung gemäß Absatz 1 Satz 3 zur Verfügung stehen. Als ein Verfahren zur sicheren Anmeldung muss der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes genutzt werden können.

§ 5

Postfach- und Versanddienst

(1) Der akkreditierte Diensteanbieter hat dem Nutzer ein sicheres elektronisches Postfach und einen sicheren Versanddienst für elektronische Nachrichten anzubieten. Hierzu wird dem Nutzer eine De-Mail-Adresse für elektronische Post zugewiesen, welche enthalten muss:

1. bei natürlichen Personen im lokalen Teil deren Nachnamen und auf Verlangen des Nutzers einen oder mehrere Vornamen oder einen Teil des oder der Vornamen (Hauptadresse),
2. bei juristischen Personen, Personengesellschaften oder öffentlichen Stellen im Domänenteil eine Bezeichnung, welche in direktem Bezug zu deren Firma, Namen oder sonstiger Bezeichnung stehen sollte .

Im Domänenteil der De-Mail-Adresse [kann/muss] außerdem eine für alle De-Mail-Adressen einheitliche Kennzeichnung enthalten sein.

Kommentar [KJ1]: Dieser Satz wird im Rahmen der weiteren Abstimmung mit Ressorts, Ländern und Verbänden höchstwahrscheinlich zu kontroversen Diskussionen führen, da hier aus verschiedenen Gründen unterschiedliche Auffassungen bestehen, die dem BMI bereits bekannt sind. Im Verlauf der Ressorts-, Länder- und Verbändebeteiligung sollen weitere Argumente gesammelt werden, auf deren Basis besser bewertet werden kann, ob eine einheitliche Kennzeichnung im Domänenteil vorgesehen werden kann oder muss oder ob hierauf nicht auch verzichtet werden kann. Der Satz ist als ein erster Textvorschlag seitens des federführenden Ressorts BMI anzusehen, eine Entscheidung z.B. dahingehend, ob dies eine „Kann“ oder eine „Muss“-Regelung ist, soll damit noch nicht verbunden sein.

(2) Der akkreditierte Diensteanbieter kann dem Nutzer auf Verlangen pseudonyme De-Mail-Adressen zur Verfügung stellen, soweit es sich bei dem Nutzer um eine natürliche Person handelt. Die Inanspruchnahme eines Dienstes 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.

(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, eine sichere Anmeldung in der Nachricht so bestätigen zu lassen, dass die Unverfälschtheit der Bestätigung jederzeit nachprüfbar ist.

(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 enthalten:
1. die De-Mail-Adresse 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 Nachricht.

Der akkreditierte Diensteanbieter des Senders hat die Versandbestätigung mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

(8) Auf Antrag des Senders wird der Zugang einer Nachricht in das Postfach des Empfängers bestätigt. Hierbei wirken der akkreditierte Diensteanbieter des Senders und der akkreditierte Diensteanbieter des Empfängers zusammen. Der akkreditierte Diensteanbieter des Empfängers erzeugt eine Zugangsbestätigung. Die Zugangsbestätigung muss enthalten:
1. die De-Mail-Adresse 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 Zugangsbestätigung erzeugt und
4. die Prüfsumme der Nachricht.

Der akkreditierte Diensteanbieter des Empfängers hat die Zugangsbestätigung mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

(9) Ist eine öffentliche Stelle, welche zur förmlichen Zustellung im Sinne von Absatz 6 berechtigt ist, Senderin einer Nachricht, so kann sie die Erstellung einer Abholbestätigung verlangen. Aus der Abholbestätigung ergibt sich, dass die Nachricht in das Postfach des Empfängers eingelegt wurde und sich der Empfänger danach an seinem De-Mail-Konto 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 enthalten:
1. die De-Mail-Adresse 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 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 Nachricht.

Der akkreditierte Diensteanbieter des Empfängers hat die Abholbestätigung mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

(10) Der akkreditierte Diensteanbieter stellt sicher, dass Nachrichten, für die eine Zugangsbestätigung nach Absatz 8 oder eine Abholbestätigung nach Absatz 9 erteilt werden, durch den Empfänger ohne Vornahme einer sicheren Anmeldung nach § 4 erst 90 Tage nach Eingang gelöscht werden können.

(11) Auf Antrag des Nutzers, soweit es sich um eine natürliche Person handelt, bietet der akkreditierte Diensteanbieter an, dass eine Kopie aller an die De-Mail-Adresse des Nutzers

adressierte Nachrichten an eine zuvor vom Nutzer angegebene De-Mail-Adresse (Weiterleitungsadresse) weitergeleitet wird, ohne dass der Nutzer an seinem De-Mail-Konto angemeldet sein muss (automatische Weiterleitung). Der Nutzer kann den Dienst automatische Weiterleitung jederzeit zurücknehmen. Um Einstellungen an dem Dienst automatische Weiterleitung vornehmen zu können, muss der Nutzer sicher im Sinne von § 4 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 Dritten sicher elektronisch bestätigen zu lassen.

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

(3) Die zuständige Behörde kann eine Sperrung eines Identitätsdatums anordnen, wenn Tatsachen die Annahme rechtfertigen, dass das Identitätsdatum aufgrund 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, wenn dem Nutzer ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne das Verlangen nicht oder nicht in zumutbarer Weise möglich ist.

(2) Der akkreditierte Diensteanbieter hat eine De-Mail-Adresse, ein Identitätsdatum oder die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen aus dem Verzeichnisdienst unverzüglich zu löschen, wenn der Nutzer dies verlangt, die Daten auf Grund falscher Angaben ausgestellt wurden, der Diensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen akkreditierten Diensteanbieter fortgeführt wird oder die zuständige Behörde die Löschung aus dem Verzeichnisdienst anordnet. Weitere Gründe für eine Löschung können vertraglich vereinbart werden.

§ 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 Ablage von Dokumenten sicher erfolgt; Vertraulichkeit, Integrität und ständige Verfügbarkeit der abgelegten Dokumente sind zu gewährleisten. 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 mit einer

dauerhaft überprüfbaren qualifizierten Signatur gesichertes Protokoll über die Einstellung und Herausnahme von Dokumenten bereitzustellen.

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 des Postfach- und Versanddienstes nach § 5, des Verzeichnisdienstes nach § 7, der Nutzung der Dokumentenablage nach § 8, der Sperrung und Auflösung des De-Mail-Kontos nach § 10, der Einstellung der Tätigkeit nach § 11, der Vertragsbeendigung nach § 12 und der Einsichtnahme nach § 13 Absatz 3 sowie über die Maßnahmen zu unterrichten, die notwendig sind, um einen unbefugten Zugriff auf das De-Mail-Konto zu verhindern.

(2) Zur Unterrichtung nach Absatz 1 sind dem Nutzer die erforderlichen Informationen in Textform mitzuteilen, deren Erhalt und Kenntnisnahme der Nutzer als Voraussetzung für die Freischaltung des De-Mail-Kontos ausdrücklich zu bestätigen 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 vorgehaltenen Daten nicht ausreichend fälschungssicher sind oder die sichere Anmeldung gemäß § 4 Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung des Anmeldevorgangs zulassen oder
3. die zuständige Behörde die Sperrung gemäß Absatz 2 anordnet.

Weitere Sperrgründe können vertraglich vereinbart werden. Der akkreditierte Diensteanbieter muss eine Sperrung anbieten, bei der der Abruf von Nachrichten möglich bleibt. 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 aufgrund 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 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 der Nutzer es verlangt oder 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 mit Ausnahme des Falles nach Satz 3 oder Absatz 2 sowie einer Auflösung nach Absatz 4 hat der akkreditierte Diensteanbieter den Eingang von Nachrichten an das Postfach eines gesperrten oder aufgelösten De-Mail-Kontos zu unterbinden und den Absender einer versandten Nachricht von deren Unzustellbarkeit unverzüglich zu unterrichten.

(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.

§ 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 wird. 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.

§ 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.

(2) Der akkreditierte Diensteanbieter hat die Dokumentation nach Absatz 1 während der Dauer des zwischen ihm und dem Nutzer bestehenden Vertragsverhältnisses sowie 30 weitere Jahre ab dem Schluss des Jahres aufzubewahren, in dem das Vertragsverhältnis endet.

(3) Dem Nutzer ist auf Verlangen Einsicht in die ihn betreffenden Daten zu gewähren.

§ 14

Jugend- und Verbraucherschutz

Der akkreditierte Diensteanbieter hat bei Gestaltung und Betrieb der De-Mail-Dienste die Belange des Jugendschutzes und des Verbraucherschutzes, insbesondere die in den von den §§ 1 und 2 des Unterlassungsklagengesetzes umfassten Vorschriften, die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb zum Schutz vor unlauteren Wettbewerbshandlungen, die geeignet sind, die Interessen von Verbrauchern spürbar zu beeinträchtigen, zu beachten.

§ 15

Datenschutz

Unbeschadet der Regelungen des Telemediengesetzes, des Telekommunikationsgesetzes und des Bundesdatenschutzgesetzes darf der akkreditierte Diensteanbieter personenbezogene Daten beim Nutzer eines De-Mail-Kontos nur erheben, verarbeiten und nutzen, soweit dies zur Bereitstellung der De-Mail-Dienste und seiner Dienste und deren Durchführung erforderlich ist.

§ 16

Auskunftsanspruch

(1) Ein akkreditierter Diensteanbieter erteilt Dritten Auskunft über Namen und Anschrift eines pseudonymen Nutzers, wenn

1. der Dritte die zur Feststellung seiner Identität notwendigen Angaben im Sinne von § 3 Absatz 2 macht und sich der Anbieter von deren Richtigkeit entsprechend § 3 Absatz 3 überzeugt hat,
2. der Dritte glaubhaft darlegt, dass er die Auskunft zur Verfolgung eines Rechtsanspruchs gegen den Nutzer benötigt und
3. das Verlangen nicht rechtsmissbräuchlich ist, insbesondere nicht allein dem Zweck dient, ein Pseudonym aufzudecken.

(2) Hat der akkreditierte Diensteanbieter dem Dritten gegenüber eine wahre Auskunft erteilt, ohne dazu nach Absatz 1 verpflichtet gewesen zu sein, haftet er dem Nutzer im Sinne von Absatz 1 nur, wenn er wusste, dass er zur Auskunftserteilung nicht verpflichtet war.

(3) Die durch die Auskunftserteilung erlangten Daten dürfen nur zu dem bei dem Ersuchen angegebenen Zweck verwendet werden.

(4) Der akkreditierte Diensteanbieter hat die Auskunftserteilung nach Absatz 1 zu dokumentieren und den Nutzer von der Erteilung der Auskunft unverzüglich und unter Benennung des Dritten zu unterrichten. 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 auskunftersuchenden Dritten, die Mitteilung über die Auskunftserteilung an den Nutzer und die jeweilige gesetzliche Zeit bei einzelnen Prozessen innerhalb der Auskunftserteilung. Die Dokumentation ist zwölf Monate aufzubewahren.

(5) Der akkreditierte Diensteanbieter kann von dem Dritten eine Erstattung für seine unmittelbaren Aufwendungen verlangen.

(6) Die nach anderen Rechtsvorschriften bestehenden Regelungen zu Auskünften gegenüber öffentlichen Stellen bleiben unberührt.

Abschnitt 4

Akkreditierung

§ 17

Akkreditierung von Diensteanbietern

(1) Diensteanbieter können 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 die Ausübung der Aufsicht über den Diensteanbieter durch die zuständige Behörde gewährleistet ist. Akkreditierte Diensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit dem Gütezeichen wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die De-Mail-Dienste erbracht. Sie dürfen sich als akkreditierte Diensteanbieter bezeichnen. Nur akkreditierte Diensteanbieter dürfen sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen und das Gütezeichen führen. Weitere Kennzeichnungen können akkreditierten Diensteanbietern vorbehalten sein.

(2) Die Akkreditierung ist nach wesentlichen Veränderungen, spätestens jedoch nach drei Jahren zu erneuern.

(3) Behörden des Bundes, der Länder und Kommunen, die geeignete Nachweise nach § 18 Absatz 2 Nummer 3 und 4 erbracht haben, erhalten auf schriftlichen Antrag das Gütezeichen nach Absatz 1.

§ 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 befinden;

4. bei Gestaltung und Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllt.

(2) Die technischen und organisatorischen Anforderungen an die Pflichten nach den § 3 bis 13 sowie nach § 16 sind nach dem Stand der Technik zu erfüllen. Der Stand der Technik ist als niedergelegt zu vermuten in der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik. Diese ist in der Anlage aufgeführt und gilt in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung. Bevor das Bundesamt für Sicherheit in der Informationstechnik wesentlichen Änderungen an der Technischen Richtlinie vornimmt, hört es den Ausschuss De-Mail-Standardisierung an.

(3) Die Voraussetzungen nach Absatz 1 werden wie folgt nachgewiesen:

1. die erforderliche Zuverlässigkeit und Fachkunde durch Nachweise über seine persönlichen Eigenschaften, sein Verhalten und seine Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben oder die persönlichen Eigenschaften, das Verhalten und die entsprechenden Fähigkeiten 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 zweihundertfünfzigtausend Euro für einen verursachten Schaden. Die Deckungsvorsorge kann erbracht werden durch
   a. eine Haftpflichtversicherung bei einem innerhalb der Mitgliedstaaten der Europäischen Gemeinschaft zum Geschäftsbetrieb befugten Versicherungsunternehmen oder
   b. eine Freistellungs- oder Gewährleistungsverpflichtung eines in einem der Mitgliedstaaten der Europäischen Gemeinschaft 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 Abs. 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 Nr. 3 durch Sicherheitszertifikate nach § 9 des Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik; das Zusammenwirken mit den anderen akkreditierten Diensteanbietern kann nur nach ausreichenden Erprobungen bestätigt werden; die Sicherheit der Dienste kann nur nach einer umfassenden Prüfung des Sicherheitskonzepts auf seine Eignung und praktische Umsetzung bestätigt werden; auf die Überprüfung der eingesetzten technischen Produkte kann verzichtet werden, wenn deren Sicherheit durch ein anerkanntes Sicherheitszertifikat nachgewiesen wird;
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 geführt dadurch, dass der antragstellende Diensteanbieter ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorlegt; der 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 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kann ergänzende Angaben anfordern; die datenschutzrechtlichen Kriterien sind in einem Kriterienkatalog definiert, der in der Verantwortung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit liegt und durch ihn im elektronischen Bundesanzeiger und zusätzlich im Internet oder in sonstiger geeigneter Weise veröffentlicht wird; der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kann für die Erteilung des Zertifikates Gebühren verlangen; .

(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 Zertifikaten im Sinne des § 18 Absatz 2 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. ungeeignete Produkte oder 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 Versanddiensts ausgestellten Zugangsbestätigungen 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 3 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 für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

Abschnitt 6

Schlussbestimmungen

§ 22

Ausschuss De-Mail-Standardisierung

Die Weiterentwicklung der technischen und organisatorischen Anforderungen an die Pflichten nach § 5 bis § 8 erfolgt unter Beteiligung der akkreditierten Diensteanbieter; dies gilt nicht, soweit es um Anforderungen geht, die das Zusammenwirken als Solches zwischen den akkreditierten Diensteanbietern oder die Sicherheit betreffen. Zu diesem Zweck wird ein Ausschuss De-Mail-Standardisierung gegründet, dem mindestens alle akkreditierten Diensteanbieter sowie das Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit angehören. Der Ausschuss tagt mindestens einmal im Jahr.

§ 23

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 3 Absatz 3 Satz 1 sich nicht vergewissert, dass die dort genannten Angaben zutreffend sind
2. entgegen § 4 Satz 2 nicht sicherstellt, dass eine sichere Anmeldung nur in den dort genannten Fällen erfolgt,
3. entgegen § 7 Absatz 2 Satz 1 dort genannte Daten nicht oder nicht rechtzeitig löscht,
4. entgegen § 10 Absatz 1 Satz 1 oder Absatz 4 Satz 1 Halbsatz 1 den Zugang zu einem De-Mail-Konto nicht oder nicht rechtzeitig sperrt oder das De-Mail-Konto nicht oder nicht rechtzeitig auflöst,
5. entgegen § 11 Absatz 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
6. entgegen § 11 Absatz 1 Satz 3 einen Nutzer nicht, nicht richtig oder nicht rechtzeitig benachrichtigt,
7. entgegen § 11 Absatz 2 nicht sicherstellt, dass die dort genannten Daten abrufbar bleiben,
8. entgegen § 12 den Zugriff auf dort genannten Daten nicht ermöglicht oder einen Hinweis nicht, nicht richtig oder nicht rechtzeitig gibt,
9. entgegen § 13 Absatz 1 eine Dokumentation nicht oder nicht richtig erstellt,
10. entgegen § 13 Absatz 2 eine Dokumentation nicht oder nicht mindestens 30 Jahre aufbewahrt oder
11. 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 3 und 4 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

Gebühren und Auslagen

(1) Für Amtshandlungen nach den §§ 17, 18 Absatz 2 Nummer 4, 19 Absatz 2 und § 20 Absatz 2 bis 4 können zur Deckung des Verwaltungsaufwands Gebühren und Auslagen erhoben werden.

(2) Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrats die gebührenpflichtigen Tatbestände, Gebührensätze sowie die Auslagenerstattung zu bestimmen und dabei feste Sätze vorzusehen. In der Rechtsverordnung kann die Erstattung von Auslagen abweichend von § 10 des Verwaltungskostengesetzes geregelt werden. Ermäßigungen und Befreiungen von Gebühren und Auslagen können zugelassen werden.

Artikel 2

Änderung der Zivilprozessordnung

§ 174 Absatz 3 der Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 29 des Gesetzes vom 17. Dezember 2008 (BGBl. I 2586) geändert worden ist, wird folgender Satz angefügt:

„Die Übermittlung kann auch über De-Mail-Dienste im Sinne von § 1 des De-Mail-Gesetzes erfolgen.“

Artikel 3

Änderung des Verwaltungszustellungsgesetzes

Das Verwaltungszustellungsgesetz vom 12. August 2005 (BGBl. I S. 2354), das zuletzt durch Artikel 9a des Gesetzes vom 11. Dezember 2008 (BGBl. I S. 2418) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) In Absatz 2 Satz 1 werden nach dem Klammerzusatz „(Post)“ ein Komma und die Wörter „einen nach § 17 des De-Mail-Gesetzes akkreditierten Diensteanbieter“ eingefügt.

   b) Absatz 3 Satz 2 wird wie folgt gefasst:

   „§ 5 Abs. 5 Satz 2 bleibt unberührt.“

2. § 5 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

„Zustellung durch die Behörde gegen Empfangsbekenntnis; elektronische Zustellung“

b) Absatz 5 wird wie folgt gefasst:

„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 nach dem Signaturgesetz zu versehen und gegen unbefugte Kenntnisnahme Dritter zu schützen.“

c) Absatz 7 wird wie folgt geändert:

aa) Satz 2 wird wie folgt gefasst:

„Ein elektronisches Dokument gilt in den Fällen des Absatzes 5 Satz 2 am dritten 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.“

bb) In Satz 3 werden die Wörter „glaubhaft macht“ durch das Wort „nachweist“ ersetzt.

cc) Satz 4 wird wie folgt gefasst: „Der Empfänger ist in den Fällen des Absatzes 5 Satz 2 vor der Übermittlung über die Rechtsfolgen nach Satz 2 und 3 zu belehren.“

3. Nach § 5 wird folgender § 5a eingefügt:

„§ 5a

Elektronische Zustellung gegen Abholbestätigung über De-Mail-Dienste

(1) Die elektronische Zustellung kann im Übrigen unbeschadet des § 5 Absatz 4 und 5 Satz 1 und 2 durch Übermittlung nach § 17 des De-Mail-Gesetzes akkreditierter Diensteanbieter gegen Abholbestätigung an das De-Mail-Postfach des Empfängers erfolgen. Bei der Zustellung nach Satz 1 findet § 5 Absatz 4 und 6 mit der Maßgabe Anwendung, dass an die Stelle des Empfangsbekenntnisses die Abholbestätigung tritt.

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

(3) Zum Nachweis der elektronischen Zustellung genügt die elektronische Abholbestätigung. Für diese gilt § 371a Absatz 2 der Zivilprozessordnung.

(4) Ein elektronisches Dokument gilt in den Fällen des § 5 Absatz 5 Satz 2 am dritten Tag nach der Absendung an das De-Mail-Postfach des Empfängers als seines hierfür eröffneten Zuganges als zugestellt, wenn 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 Satz 1 und 2 zu belehren. Zum Nachweis der Zustellung dient die elektronische Versandbestätigung oder ein Vermerk der absendenden Behörde in den Akten, zu welchem Zeitpunkt und an welchen Zugang das Dokument gesendet wurde. Der Empfänger ist über den Eintritt der Zustellungsfiktion nach Satz 1 zu benachrichtigen.

4. § 9 wird wie folgt geändert:

   a) In Absatz 1 Nummer 4 wird die Angabe „nach § 5 Abs. 5“ gestrichen.

   b) In Absatz 2 Satz 3 wird nach der Angabe „§ 5 Abs. 7 Satz 1 bis 3 und 5“ die Angabe „sowie nach § 5a Absatz 3 und 4 Satz 1, 2 und 4“ eingefügt.

   c) Dem Absatz 3 wird folgender Satz angefügt:

   „Wird das Verwaltungsverfahren über eine einheitliche Stelle nach § 71 a ff. des Verwaltungsverfahrensgesetzes abgewickelt, finden die Sätze 1 bis 6 keine Anwendung.“

Artikel 4

Änderung des Bürgerlichen Gesetzbuches

§ 312e des Bürgerlichen Gesetzbuches in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch das Gesetz vom 28. September 2009 (BGBl. I S. 3161) geändert worden ist, wird folgender Absatz 4 angefügt:

„Bedient sich ein Unternehmer zum Zwecke der Ausübung seiner vertraglichen Beziehung mit einem Kunden des De-Mail-Dienstes im Sinne des De-Mail-Gesetzes und versendet an diesen De-Mail-Nachrichten, so ist er verpflichtet, über die De-Mail-Dienste versandte De-Mail-Nachrichten des Kunden an ihn zu empfangen, soweit der Kunde dies verlangt. Insbesondere darf er De-Mail-Nachrichten seines Kunden nicht mit der Begründung ablehnen, dass der Kunde stattdessen seine Angebote im Internet wie Herunterladen von Formularen nutzen kann.“

Artikel 5

Evaluierung

Die Bundesregierung beobachtet die Entwicklung der De-Mail-Dienste und legt dar, ob und gegebenenfalls in welchen Bereichen Anpassungs- oder Ergänzungsbedarf bei den rechtlichen Rahmenbedingungen für die neuen Dienste und bei den Vorschriften über die elektronische Zustellung besteht. Hierbei wird sie insbesondere auch prüfen, ob die Einführung einer Zertifizierung von Verbraucherschutzkriterien als Voraussetzung für die Akkreditierung von Diensteanbietern geboten ist. Sie legt hierüber dem Deutschen Bundestag bei Bedarf, spätestens jedoch nach Ablauf von drei Jahren nach Inkrafttreten dieses Gesetzes einen Bericht vor.

Artikel 6

Inkrafttreten

Dieses Gesetz tritt am ersten Tag des auf die Verkündung folgenden Kalendermonats in Kraft.

Anhang zu Artikel 1

Anlage 1

Übersicht über die Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik

BSI: Technische Richtlinie TR-01201 De-Mail (TR DM)

Mit den Modulen:

Modul IT-Basisinfrastruktur (TR DM M Binfra)

Modul Postfach- und Versanddienst (TR DM M PVD)

Modul Accountmanagement (TR DM M ACM)

Modul Sicherheit (TR DM M IT-Si)

Modul Dokumentensafe (TR DM M DS)

Modul Identifizierungsdienst (TR DM M ID)

Begründung

A. Allgemeiner Teil

I. Ziel und Inhalt des Entwurfs

1. Ausgangslage

Das Gesetz verfolgt die Ziele,

- einen Rechtsrahmen zur Einführung vertrauenswürdiger De-Mail-Dienste im Internet zu schaffen, der für Diensteanbieter Rechtssicherheit schafft und ihnen ermöglicht, die Rechtsqualität der als De-Mail-Dienste erfassten Dienste im Internet zu steigern,
- für die elektronische Kommunikation im Rechts- und Geschäftsverkehr vertrauenswürdige Lösungen zu schaffen, bei denen sich die Teilnehmer der Sicherheit der Dienste, der Vertraulichkeit der Nachrichten und der Identität ihrer Kommunikationspartner sicher sein können,
- die Rechtssicherheit im elektronischen Rechts- und Geschäftsverkehr durch verbesserte Beweismöglichkeiten zu stärken,
- den rechtlichen Rahmen für eine rechtssichere Zustellung elektronischer Dokumente zu schaffen.

Das Gesetz reiht sich in die Bemühungen ein, für den elektronischen Rechts- und Geschäftsverkehr geeignete Rahmenbedingungen herzustellen, die eine vergleichbare Vertrauenswürdigkeit gewährleisten wie die auf Papier beruhende Kommunikation. Anlass des Tätigwerdens des Gesetzgebers ist u. a. die Erkenntnis, dass sich die schon lange vorhandenen Möglichkeiten, elektronische Kommunikation zu verschlüsseln, nicht haben durchsetzen können. Insoweit ist wesentliches Ziel der De-Mail-Dienste, dass diese einfach nutzbar sind und gleichzeitig ein wesentliches höheres Maß an Sicherheit gegenüber der herkömmlichen E-Mail-Kommunikation mit sich bringen. Zugleich wird die Möglichkeit der Nachweisbarkeit darüber, von wem eine elektronische Nachricht stammt und dass sie an den Empfänger, an den sie gehen sollte, tatsächlich gelangt ist, erheblich verbessert. Grundlage der Nutzung der De-Mail-Dienste im elektronischen Rechts- und Geschäftsverkehr ist dabei stets die freiwillige Entscheidung der Nutzer. Sonderanwendungen werden durch dieses Gesetz nicht berührt.
Die Freiwilligkeit der Nutzung von De-Mail gilt für alle Nutzer: natürliche Personen (also auch in ihrer Eigenschaft als Verbraucher im Sinne von § 13 des Bürgerlichen Gesetzbuches) juristische oder Personengesellschaften (auch in ihrer Eigenschaft als Unternehmer im Sinne von § 14 des Bürgerlichen Gesetzbuches). De-Mail ist umso erfolgreicher, je mehr Nutzer gewonnen werden können. Für die Seite von Unternehmen als „Massenversender“ ergibt sich der Nutzen von De-Mail daraus, dass sie durch Versendung per De-Mail gegenüber der Versendung per physischer herkömmlicher Post Kosten sparen. Für den Bürger ergibt sich der Nutzen daraus, dass sie rechtsgeschäftlich relevanten Schriftverkehr zukünftig elektronisch vornehmen können und dabei nur noch ein Konto benötigen. Verbraucher müssen sich also z. B. nicht mehr an Web-Portalen verschiedenster Art anmelden. Voraussetzung hierfür ist allerdings, dass die Betreiber dieser Web-Portale, in der Regel Unternehmer, „Massenversender“, ihre Kunden, die sie per De-Mail erreichen können, nicht wieder auf ihre Portale verweisen, sondern diesen anbieten, deren – der Kunden/Verbraucher – Post ebenfalls elektronisch per De-Mail anzunehmen. Dass es diese Alternative überhaupt gibt, ergibt sich daraus, dass das Erfordernis der „Textform“ nach § 126b BGB sowohl durch eine übersandte E-Mail als auch durch das tatsächliche Downloaden von Dokumenten auf Web-Portalen seitens des Empfängers gewahrt ist (vgl. Palandt, Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, Rn. 3 zu § 126b). Auf ihrem De-Mail-Konto können Bürger als Verbraucher rechtsgeschäftlich relevante Kommunikation empfangen (dies ist das Interesse der „Massenversender“) aber auch versenden (dies ist das Interesse der natürlichen Person als Verbraucher, Kunde eines Massenversenders). Um eine rasche Akzeptanz beim Bürger zu erreichen, sollten im Sinne einen Gegenseitigkeitsprinzips Unternehmen darum bemüht sein, dass sie, wenn sie mit

ihren Kunden per De-Mail kommunizieren, genauso den Empfang von De-Mail-Nachrichten ihrer Kunden akzeptieren. Zur Erreichung dieses Zieles soll zum Einen der akkreditierte Diensteanbieter seine Nutzer im Rahmen seiner Aufklärungspflichten nach Art. 1 § 9 darüber informieren, dass sie dieses Recht bei den Unternehmen, bei denen sie Kunden sind, einfordern. Zum anderen wird durch Art. [3a] unter dem Aspekt des Verbraucherschutzes das BGB angepasst, um ein solches Gegenseitigkeitsprinzip zu verankern.

Das Verhältnis zum Signaturgesetz stellt sich wie folgt dar: Die De-Mail-Dienste stellen keine Alternative zur qualifizierten elektronischen Signatur nach Signaturgesetz dar. Die qualifizierte elektronische Signatur nach Signaturgesetz stellt insbesondere das Äquivalent zur handschriftlichen Unterschrift dar und dient damit der Erfüllung eines im Einzelfall erforderlichen Schriftformerfordernisses im Sinne von § 126a des Bürgerlichen Gesetzbuches (BGB), § 3a des Verwaltungsverfahrensgesetzes (VwVfG), § 36a des Ersten Buches Sozialgesetzbuch (SGB I) und § 87a der Abgabenordnung (AO). Mit den De-Mail-Diensten wird hingegen eine Plattform bereitgestellt, die – im Gegensatz zur herkömmlichen E-Mail-Kommunikation – eine sichere und nachvollziehbare Kommunikation schafft. Die bis dato fehlende Nachweisbarkeit der elektronischen Kommunikation wird mit De-Mail nunmehr möglich, da der Versand bzw. der Empfang von De-Mails nachgewiesen werden kann und die Identität der Kommunikationspartner gesichert ist. Ergänzend kann die qualifizierte elektronische Signatur vom Nutzer z. B. in den Fällen eingesetzt werden, wenn ein per De-Mail versendetes Dokument einem Schriftformerfordernis unterliegt und daher nach § 126a BGB, § 3a VwVfG, § 36a SGB I oder § 87a AO mit einer qualifizierten elektronischen Signatur nach Signaturgesetz versehen werden muss.

Damit die Teilnehmer des Rechts- und Geschäftsverkehrs die Vertrauenswürdigkeit eines Angebots von De-Mail-Diensten erkennen können, wird die Möglichkeit geschaffen, diese durch eine Akkreditierung vertrauenswürdiger Diensteanbieter bestätigen zu lassen und durch ein Gütezeichen nachzuweisen. An diesen Nachweis können andere Gesetze bestimmte Rechtsfolgen knüpfen, die eine solche Vertrauenswürdigkeit voraussetzen. An eine vorgenommene Akkreditierung knüpft beispielsweise die Beleihung an, deren der Diensteanbieter für die Ausführung elektronischer Zustellungen und die Abgabe entsprechender Bestätigungen bedarf. In der Praxis noch wichtiger werden die faktischen Schlussfolgerungen sein, die die Teilnehmer des Rechts- und Geschäftsverkehrs aufgrund der vorgeprüften und nachgewiesenen Vertrauenswürdigkeit der Diensteanbieter ziehen. Auf die nachgewiesene Vertrauenswürdigkeit können auch Beweisregelungen aufbauen.

Das Gesetz ist wesentlich für die Akzeptanz und Durchsetzung der De-Mail-Dienste, deren Förderung in der 16. Wahlperiode Bestandteil der High-Tech-Strategie der Bundesregierung, des E-Government-Programms 2.0 und des in der Kabinettklausur in Meseberg beschlossenen 12-Punkte-Plans für ein bürgerfreundliches Deutschland war und auch von der Bundesregierung in der 17. Wahlperiode weiter gefördert wird.

2. Gründe für sichere De-Mail-Dienste

Die unter einem De-Mail-Dienst angebotenen Dienstleistungen eines Diensteanbieters ermöglichen es, rechtssicher im Kommunikationsraum Internet zu handeln. Durch das Angebot einer sicheren Anmeldung kann ein Anscheinsbeweis für das tatsächliche Handeln eines Nutzers erbracht werden. Ein Postfach- und Versanddienst ermöglicht eine sichere Zustellung und einen sicheren Empfang. Der mit dem De-Mail-Dienst verbundene Identitätsbestätigungsdienst eröffnet dem Nutzer die Möglichkeit, sich – angepasst an seine Bedürfnisse – Dritten gegenüber sicher zu authentisieren. Eine sichere Dokumentenablage, die es den Nutzern ermöglicht, wichtige elektronische Dateien unter Erhalt der Vertraulichkeit gegen Verlust zu sichern, rundet das Angebot von De-Mail-Diensten ab. Während es sich beim Postfach- und Versanddienst um einen Dienst handelt, den der akkreditierte Diensteanbieter anbieten muss, bleibt ihm dies bezüglich des Identitätsbestätigungsdienstes und des Dienstes Dokumentenablage freigestellt.
Bei den De-Mail-Diensten handelt es sich um Dienstleistungen, die sowohl dem Telekommunikations- wie auch dem Telemediensektor zuzuordnen sind. E-Mail-Dienste sind

Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, also neben der Übertragungsdienstleistung noch eine inhaltliche Dienstleistung anbieten. Diese sind zugleich Telemediendienste und fallen damit mit Ausnahme der Vorschriften zum Datenschutz auch unter das TMG und die darin enthaltenen Regeln zum Herkunftslandprinzip, zur Zugangsfreiheit und zur Haftungsprivilegierung. Dieser Regelungszusammenhang ist europarechtlich vorgegeben, denn diese Dienste fallen als Dienste der Informationsgesellschaft und zugleich elektronische Kommunikationsdienste unter die E-Commerce-Richtlinie wie auch unter die TK-Rahmenrichtlinie (vgl. hierzu die Ausführungen im Gesetzentwurf der BReg zum Telemediengesetz, BT-Drs. 16/3078, S. 13). Insofern ergeben sich für den Versand von De-Mails keine Besonderheiten. Darüber hinausgehende Dienste der De-Mail-Dienste, die in keinem unmittelbaren Zusammenhang mit dem Nachrichtentransport stehen, sind ebenfalls als Telemediendienst einzuordnen (insbesondere die Dienste nach § 6 und § 8).

Um den Wettbewerb und die Verbreitung von De-Mail-Diensten zu fördern, sollen Diensteanbieter in erster Linie private Unternehmen sein. Gleichwohl steht es auch Behörden frei, im zulässigen Rahmen De-Mail-Dienste anzubieten.

Entscheidende Voraussetzung für den Erfolg von De-Mail-Diensten ist das Vertrauen der Öffentlichkeit in ihre Vertrauenswürdigkeit. Notwendig ist daher, dass Sicherheit und Datenschutz nicht nur behauptet, sondern nachgewiesen werden. Aufgrund seiner Schutz- und Gewährleistungsfunktion kommt dem Staat die Aufgabe zu, der Wirtschaft ein entsprechendes Nachweisverfahren anzubieten. Das Gesetz ermöglicht daher eine Akkreditierung.

Diese ermöglicht Diensteanbietern, ihre Dienste als De-Mail-Dienste wirksam aufzuwerten. Sie können die Qualität ihrer Dienste in einem rechtssicheren Rahmen mit definierten Anforderungen verbessern und die Erfüllung dieser Anforderungen gegenüber ihren Kunden nachweisen. Basis dieser Nachweise ist ein technisches Konzept, das hinter den De-Mail-Diensten steht. Dieses sollte regelmäßig im Hinblick auf sinnvolle technische Weiterentwicklungen überprüft und angepasst werden. Hierbei sollten regelmäßige Abstimmungen insbesondere zwischen den für die Aufstellung und Pflege der Anforderungen für die Bereiche Funktionalität, Interoperabilität, Sicherheit und Datenschutz verantwortlichen Stellen und den akkreditierten Diensteanbietern erfolgen.

Dieses Gesetz schließt das Angebot von den De-Mail-Diensten entsprechenden Diensten im Internet ohne Nachweis ausreichender Vertrauenswürdigkeit nicht aus. Es können also auch nicht nach den Regelungen des De-Mail-Gesetzes akkreditierte Diensteanbieter Dienste, die den De-Mail-Diensten entsprechen, anbieten.

Um den Verwaltungsaufwand für die Akkreditierung zu reduzieren, wird von der zuständigen Behörde weitgehend nur geprüft, ob die Voraussetzungen der Akkreditierung durch Zertifikate zuverlässiger und kompetenter Stellen nachgewiesen werden.

Für juristische Personen und andere Organisationen besteht ein praktisches Bedürfnis, dass ihre Mitarbeiter oder Mitglieder unter Nutzung einer gleichförmigen De-Mail-Adresse am elektronischen Rechtsverkehr teilnehmen können. Die Anbindung solcher Organisationen kann auf verschiedene Weise geschehen. So kann die Organisation bei einem akkreditierten Diensteanbieter für eine Vielzahl von natürlichen Personen jeweils ein De-Mail-Konto anmelden. Sie kann dabei zur Entlastung des Diensteanbieters für diesen die nach § 3 des De-Mail- Gesetzes erforderliche Identifizierung der einzelnen Nutzer als Dritter im Sinne von § 18 Absatz 3 des De-Mail- Gesetzes übernehmen. Ebenso besteht die Möglichkeit, dass die an der Anbindung ihrer Mitarbeiter oder Mitglieder interessierte Organisation selbst im Rechtsverkehr als Diensteanbieter auftritt und bei der zuständigen Behörde eine Akkreditierung nach § 17 des De-Mail- Gesetzes beantragt. In diesem Fall kann ein anderer akkreditierter Diensteanbieter im Innenverhältnis für die Organisation die ihr nach dem De-Mail- Gesetz obliegenden Pflichten übernehmen.

Da mit der Akkreditierung die Vertrauenswürdigkeit des Angebots von De-Mail-Diensten bestätigt und durch ein Gütezeichen nachgewiesen wird, ist es möglich, weitergehende Rechtsfolgen an die angebotenen Dienste zu knüpfen, als dies ohne Akkreditierung der Fall wäre. So ist sie ausdrückliche Voraussetzung für die Übermittlung nach dem vorgeschlagenen § 174 Absatz 3 Satz 4 der Zivilprozessordnung oder für die elektronische Zustellung nach dem vorgeschlagenen § 5a des Verwaltungszustellungsgesetzes. Gleichzeitig sind mit der Akkreditierung aber auch nicht ausdrücklich geregelte Rechtsfolgen angestrebt. Dazu zählt der Anscheinsbeweis bei einer sicheren Anmeldung, aber auch die Annahme einer Zugangseröffnung gemäß § 3a Absatz 1 des Verwaltungsverfahrensgesetzes bei der Nutzung einer De-Mail-Adresse in der Kommunikation mit staatlichen Stellen.

Die nachfolgenden Vorschriften enthalten keine Regelungen zur Entgeltlichkeit der angebotenen Dienste. Die Pflicht des Diensteanbieters, diese Dienste dem Nutzer anzubieten, schließt die Entgeltlichkeit der Dienste nicht aus.

3. Verfassungsmäßigkeit

Das Gesetz ist verfassungsrechtlich zulässig. Die Akkreditierung der Diensteanbieter ist keine Voraussetzung, um diese Dienste am Markt anbieten zu dürfen, sondern lediglich eine Bestätigung, dass eine bestimmte geprüfte Vertrauenswürdigkeit der Dienste vorliegt. Die Akkreditierung ist daher eine Regelung der Berufswahl, die in den Schutzbereich des Art. 12 Absatz 1 des Grundgesetzes eingreift. Die Vorabprüfung der Anforderungen an sichere De-Mail-Dienste durch die Akkreditierung ist jedoch erforderlich, um die Vertrauenswürdigkeit der Dienste sicherzustellen und das Anknüpfen weiterer Rechtsfolgen zu ermöglichen. Ohne diese Gewährleistung der Vertrauenswürdigkeit können die De-Mail-Dienste ihre Aufgabe nicht erfüllen. Die Diensteanbieter können die Dienste dagegen auch ohne Akkreditierung betreiben, sie profitieren jedoch dann nicht von der nachgewiesenen Sicherheit. Die Regelungen des De-Mail- Gesetzes sind damit auch verhältnismäßig. Ferner ist der verfassungsrechtliche Grundsatz fairer Verfahrensführung gewahrt, weil durch die individuelle Beantragung der Eröffnung eines De-Mail Kontos durch den Bürger (vgl. Art. 1 § 3 Absatz 1) dessen Wunsch nach Nutzung des De-Mail-Dienstes deutlich wird.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz für das De-Mail-Gesetz mit seinen Regelungen über das Akkreditierungsverfahren und die Anforderungen an das Angebot von De-Mail-Diensten ergibt sich aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Abs. 1 Nr. 11 Grundgesetz). Die Berechtigung des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich aus Artikel 72 Abs. 2 Grundgesetz. Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte, z.B. unterschiedliche Voraussetzungen für die Akkreditierung von Diensteanbietern von De-Mail-Diensten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Die Kommunikation über De-Mail-Dienste zeichnet sich gerade durch einen grenzüberschreitenden Bezug aus; die Anknüpfung von Rechtsfolgen an die Vorabprüfung der Dienste verlangt ebenfalls einheitliche Rahmenbedingungen.

Die Gesetzgebungskompetenz für die Änderung der Zivilprozessordnung (Artikel 2) und des Bürgerlichen Gesetzbuches (Artikel 4) ergibt sich aus Artikel 74 Absatz 1 Nr. 1 Grundgesetz. Die Änderungen des Verwaltungszustellungsgesetzes (Artikel 3) kann der Bund als Annex zur Sachkompetenz mitregeln.

III. Vereinbarkeit mit dem Recht der Europäischen Union

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar. Die europarechtliche Zulässigkeit der Akkreditierung und der Regulierung von De-Mail-Diensten bemisst sich nach der allgemeinen Niederlassungs- und Dienstleistungsfreiheit des EG-Vertrages (Artikel 43 ff. und Artikel 49 ff.), die durch die bereits bei der Rechtsetzung zu beachtende Dienstleistungsrichtlinie (Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt - DLRL) konkretisiert werden. Die DLRL ist auf die Regelungen des De-Mail- Gesetzes (Art. 1) – mit Ausnahme von § 19 – allerdings nicht anwendbar. Dies ergibt sich aus Art. 2 Absatz 2 Buchst i) DLRL, wonach die DLRL auf solche Tätigkeiten keine Anwendung findet, die im Sinne des Art. 45 EGV mit der Ausübung öffentlicher Gewalt verbunden sind. Öffentliche Gewalt im Sinn des Art. 45 EGV erfasst die Möglichkeit, dem Bürger gegenüber von Sonderrechten, Hoheitsprivilegien und Zwangsbefugnissen Gebrauch zu machen. Da ein akkreditierter Diensteanbieter bei der förmlichen Zustellung eine elektronische Abholbestätigung erzeugt, die die Beweiskraft einer öffentlichen Urkunde hat, setzt dies eine Übertragung hoheitlicher Befugnisse voraus. Diese erfolgt durch die in Art. 1 § 5 Abs. 6 geregelte Beleihung. Daher ist konkret diese Regelung vom Anwendungsbereich der DLRL ausgenommen. Die Pflicht des akkreditierten Diensteanbieters, förmliche Zustellungen auszuführen und dafür elektronische Abholbestätigungen zu erzeugen, ist zugleich wesentlicher Bestandteil des (Pflichtdienstes) Postfach- und Versanddienstes, dieser wiederum ist als Pflichtdienst der wesentlichste Bestandteil und eigentliche Kern der De-Mail-Dienste. Die Tätigkeit des Betreibens von De-Mail-Diensten der akkreditierten Diensteanbieter ist damit insgesamt vom Anwendungsbereich der DLRL ausgenommen. Da die Beleihung automatisch mit der Akkreditierung erfolgt, sind somit auch sämtliche Regelungen, die die Akkreditierung der Diensteanbieter betreffen, vom Anwendungsbereich der DLRL ausgenommen.

Obwohl die DLRL im Wesentlichen auf die De-Mail-Dienste nicht anwendbar ist, sind die De-Mail-Dienste bei der Umsetzung der DLRL von Bedeutung. Für die Verwaltung ist es im Rahmen der Umsetzung der DLRL erforderlich, dass die elektronische Kommunikation zuverlässig funktioniert, einen sicheren Zugang sowie eine klare Identitätszuordnung ermöglicht. Dies vor dem Hintergrund, dass der Dienstleister nach der Richtlinie einen Anspruch auf elektronische Verfahrensabwicklung hat (Art. 8 Abs.1 DLRL). De-Mail-Dienste können dabei eine wichtige Rolle spielen, da sie für die deutsche Verwaltung eine rechtssichere Lösungsmöglichkeit bei der Realisierung der elektronischen Kommunikation darstellen. Durch De-Mail-Dienste können derzeitige Schwierigkeiten technischer Natur bei der elektronischen Zustellung gelöst werden. Darüber hinaus werden die Möglichkeiten der Behörde – sollte sie sich für die Nutzung eines De-Mail-Dienstes entscheiden –, die Zustellung eines elektronischen Dokumentes im Streitfall zu beweisen, erheblich verbessert. Damit werden die mit dem Vierten Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 11. Dezember 2008 (BGBl. I S. 2418) zur Umsetzung der DLRL geschaffenen zustellungsrechtlichen Vorschriften, die an die heute bestehenden technischen Möglichkeiten der Kommunikation mit E- Mails anknüpfen, fortentwickelt

IV. Kosten

<u>Haushaltsausgaben ohne Vollzugsaufwand</u>

Haushaltsausgaben ohne Vollzugsaufwand entstehen nicht.

Vollzugsaufwand

Für den Betrieb der De-Mail-Dienste sind in der Regel private Diensteanbieter vorgesehen. Gleichwohl steht es auch Behörden frei, im zulässigen Rahmen De-Mail-Dienste anzubieten. Verwaltungsaufwand entsteht insbesondere durch die Akkreditierung der De-Mail-Diensteanbieter und die Aufsicht über diese. Diese Aufgaben sollen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wahrgenommen werden. Die diesbezüglich neu zu schaffenden Befugnisse des BSI sind mit einem entsprechenden Vollzugsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der Inanspruchnahme des Akkreditierungsverfahrens durch potentielle De-Mail-Diensteanbieter abhängig und daher nur schwer zu beziffern.

Beim BSI besteht aufgrund des De-Mail-Gesetzes ein Aufwand an ca. 8 zusätzlichen Planstellen/Stellen mit Mehrkosten in Höhe von jährlich rund 525.000 Euro. Beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) besteht ein Bedarf in Höhe von 3 zusätzlichen Planstellen/Stellen mit Mehrkosten in Höhe von jährlich rund 263.000 Euro. Dieser ergibt sich aus der für den BfDI neuen Aufgabe gem. § 18 Absatz 3, die vom an einer Akkreditierung interessierten Diensteanbieter vorzulegenden Nachweise zur Erfüllung der datenschutzrechtlichen Anforderungen zu prüfen und auf Antrag des Diensteanbieters ein Zertifikat zu erteilen. Außerdem ist der BfDI für die den Nachweisen zugrundeliegenden datenschutzrechtlichen Kriterien verantwortlich. Die zusätzlichen Stellen und der Mehraufwand beim BSI und beim BfDI sind aus dem Gesamthaushalt zu finanzieren. Eine Kompensation aus dem Einzelplan 06 ist nicht möglich. Der beim BSI und BfDI entstehende Mehraufwand bei den Sachkosten wird zum Teil durch noch festzulegende Gebühren für das jeweilige Verfahren (u. a. Akkreditierungsverfahren bzw. Zertifizierungsverfahren) gedeckt. Im Übrigen werden die Sachkosten grundsätzlich aus dem Einzelplan erwirtschaftet.

Kosten zur Anpassung von Verfahren der Verwaltung an die Nutzung von De-Mail-Diensten können nicht benannt werden. Sie treffen Bund, Länder und Kommunen gleichermaßen. Langfristig können Verwaltungskosten durch die Verbreitung und Nutzung der De-Mail-Dienste jedoch gesenkt werden und elektronische Geschäftsprozesse, deren Risiko sinkt, kostengünstiger angeboten werden. Die Verwaltung kann durch Nutzung der De-Mail-Dienste insbesondere den Anteil der mit hohen Porto-, Material- und Prozesskosten versehenen Papierpost reduzieren (siehe V. Nutzenbetrachtungen).

Informationspflichten und Kosten für die Wirtschaft

Den Diensteanbietern entstehen Kosten durch die Durchführung des Akkreditierungsverfahrens und die Maßnahmen zur Erfüllung der Voraussetzungen der Akkreditierung. Den Kosten steht jedoch der Gegenwert einer nachweisbaren Dienstequalität und Sicherheit gegenüber.

Die neuen Informationspflichten für die Wirtschaft gelten für Dienstanbieter, die De-Mail-Dienste anbieten. Im Rahmen des Ex-Ante-Verfahrens wurden die Bürokratiekosten der Wirtschaft auf rund 2,5 Mio. Euro beziffert. Das Einsparungspotenzial bei den Bürokratiekosten der Wirtschaft aus Informationspflichten kann allein aufgrund der zu erwartenden Portokosteneinsparungen beträchtlich sein, ist aber zur Zeit noch nicht bezifferbar (siehe auch V. Nutzenbetrachtungen).

Den folgenden Berechnungen liegt die Annahme zu Grunde, dass sich im ersten Jahr nach Inkrafttreten des Gesetzes drei, im zweiten Jahr ebenfalls drei, im dritten Jahr weitere vier und in den beiden folgenden Jahren je weitere fünf Diensteanbieter akkreditieren lassen werden und sich danach ein relativ konstanter durchschnittlicher Wert von 20 Diensteanbietern am Markt ergibt. Eine weitere Annahme ist, dass die Diensteanbieter bereits ähnliche Dienste im E-Mail-Bereich etabliert haben, so dass nur die ggf. notwendigen

zusätzlichen Infrastrukturkomponenten sowie die eigentliche Prüfung und Akkreditierung im Sinne des Gesetzes betrachtet werden.

Im Einzelnen:

- Akkreditierung von Diensteanbietern

  Nach § 17 Abs. 1 können sich Diensteanbieter auf schriftlichen Antrag von der zuständigen Behörde akkreditieren lassen. Dafür müssen vom Diensteanbieter bestimmte Voraussetzungen nachgewiesen werden:

  - Zuverlässigkeit und Fachkunde durch entsprechende Zeugnisse oder Nachweise (§ 18 Absatz 2 Nr. 1)
    Die dadurch entstehenden Kosten sind gering und können in den weiteren Betrachtungen vernachlässigt werden.

  - Ausreichende Deckungsvorsorge durch den Abschluss einer Versicherung oder die Freistellungs- oder Gewährleistungsverpflichtung eines Kreditunternehmens (§ 18 Absatz 2 Nr. 2).
    Für die Deckungsvorsorge durch Abschluss einer entsprechenden Versicherung wird von jährlichen Kosten für die Diensteanbieter in Höhe von 100.000 € ausgegangen. Damit ergeben sich über die ersten fünf Jahre gemittelte jährliche Gesamtkosten in Höhe von 1,080 Mio. €.

  - Erfüllung der Pflichten nach §§ 3 bis 13 sowie § 16, Zusammenwirken mit anderen akkreditierten Diensteanbietern (Interoperabilität), ständige Verfügbarkeit, sicheres Erbringen der Dienste durch Sicherheitszertifikate (§ 18 Absatz 2 Nummer 3) und Erfüllung der datenschutzrechtlichen Anforderungen (§ 18 Absatz 2 Nummer 4).
    Dafür sind folgende Prüfungen erforderlich:
    - Interoperabilität der angebotenen Dienste
    - IT-Sicherheit der eingesetzten sicherheitsrelevanten Hard- und Softwarekomponenten
    - IT-Sicherheit nach ISO 27001 auf der Basis von IT-Grundschutz (für Organisation und Prozesse)
    - Datenschutz

    Die Kosten für die Prüfungen hängen insbesondere von den eingesetzten Produkten ab. Sind diese bereits zertifiziert, so fallen keine Kosten an. Dies gilt ebenfalls für den Bereich IT-Sicherheit nach ISO 27001. Ist ein Großteil der IT-Infrastruktur des Diensteanbieters bereits zertifiziert, so reduzieren sich die Kosten erheblich.
    Berücksichtigt man ferner auch die Kosten für die eigentliche Akkreditierung durch die zuständige Stelle, so werden sich die Kosten in einem Bereich von 65.000 € bis 535.000 € bewegen. Für die weiteren Betrachtungen wird der arithmetische Mittelwert in Höhe von 300.000 € pro Dienstanbieter verwendet.
    Die Akkreditierung ist nach wesentlichen Veränderungen, spätestens jedoch nach drei Jahren zu wiederholen (§ 17 Absatz 2). Für diesen Prozess werden Kosten in Höhe von einem Drittel der initialen Akkreditierung, also 100.000 € angenommen.
    Unter der Annahme, dass sich in den ersten fünf Jahren insgesamt 20 Diensteanbieter akkreditieren lassen und von den 10 in den ersten drei Jahren akkreditierten Diensteanbietern sechs die Re-Akkreditierung durchlaufen, betragen die durchschnittlichen jährlichen Kosten für die Wirtschaft 1,32 Mio. €.
    Wenn es die Marktentwicklung für De-Mail-Dienste in den nächsten Jahren erlaubt, wird es spezialisierte Provider geben, die für weitere Diensteanbieter eine bereits geprüfte IT-Infrastruktur bereitstellen. In diesem Fall werden die Akkreditierungskosten deutlich unter 300.000 € liegen.

- Betrieb von De-Mail-Diensten

Im Rahmen des Betriebes von De-Mail-Diensten gelten für die akkreditierten Diensteanbieter folgende Informationspflichten:

- Nach § 9 hat der akkreditierte Diensteanbieter den Nutzer vor der erstmaligen Nutzung des De-Mail-Dienstes über die notwendigen Maßnahmen zu unterrichten, um einen unbefugten Zugriff auf De-Mail-Dienste zu verhindern, und auf mögliche Rechtsfolgen der Nutzung von De-Mail-Diensten hinzuweisen. Dazu ist dem Nutzer eine Belehrung in Textform zu übermitteln.
  Diese Belehrung erfolgt automatisiert im Rahmen der Eröffnung eines De-Mail-Kontos und ist mit keinen nennenswerten Kosten für die Wirtschaft verbunden.

- Nach § 13 Absatz 2 hat der akkreditierte Diensteanbieter die Dokumentation während der Dauer des zwischen ihm und dem Nutzer bestehenden Vertragsverhältnisses sowie 30 weitere Jahre ab dem Schluss des Jahres aufzubewahren, in dem das Vertragsverhältnis endet.
  Die Aufbewahrung der Dokumentation der Vertragsverhältnisse mit den Nutzern (in elektronischer oder Papierform) über einen Zeitraum von 30 Jahren ist mit Archivierungskosten verbunden. Bei einer durchschnittlichen Anzahl von 1,25 Mio. Nutzern pro Dienstanbieter ist von jährlichen Kosten in Höhe von ca. 15.000 € auszugehen. Bei drei Dienstanbietern im ersten Jahr, drei weiteren im zweiten, vier zusätzlichen im dritten sowie jeweils fünf weiteren im vierten und fünften Jahr ergeben sich durchschnittliche Archivierungskosten von ca. 162.000 € pro Jahr.

- Gemäß § 13 Absatz 3 ist dem Nutzer auf Verlangen Einsicht in die ihn betreffenden Daten zu gewähren.
  Diese Daten stehen innerhalb der sowieso zu etablierenden De-Mail-Konto-Management-Dienste elektronisch zur Verfügung und können dem Nutzer ohne weiteren Aufwand auf Verlangen zur Verfügung gestellt werden.

- Nach § 16 erteilt ein akkreditierter Diensteanbieter unter bestimmten Voraussetzungen Auskunft über Namen und Anschrift eines Nutzers. Insbesondere hat der Dritte glaubhaft darzulegen, dass er die Auskunft zur Verfolgung eines Rechtsanspruches benötigt. Darüber hinaus hat der akkreditierte Diensteanbieter die Auskunftserteilung zu dokumentieren und den Nutzer darüber zu unterrichten.
  Eine solche Auskunftserteilung ist insbesondere dann erforderlich, wenn einem Dritten (z.B. einem Onlineshop) von einem Nutzer lediglich die (pseudonyme) De-Mail-Adresse bekannt ist und der Dritte zur Durchsetzung eines Rechtsanspruchs (z.B. auf Zahlung eines bestimmten Geldbetrages) Namen und Anschrift benötigt.
  Für Antragsprüfung, Auskunftserteilung und Unterrichtung des Nutzers werden jeweils 10 Min. mit Arbeitskosten von 30,00 €/Stunde veranschlagt, also 5,00 € pro Fall. Unter der Annahme, dass dies pro Jahr bei einem Prozent der Nutzer jeweils einmal erforderlich ist, und einer Entwicklung der Nutzerzahlen wie oben aufgeführt, ergeben sich jährliche Kosten für die Wirtschaft in Höhe von ca. 540.000 € in den ersten fünf Jahren. Nach § 16 Absatz 4 kann der Diensteanbieter von dem Dritten eine Erstattung für seine unmittelbaren Aufwendungen verlangen.

- <u>Einstellung der Tätigkeit eines akkreditierten Diensteanbieters</u>

  Nach § 11 Absatz 1 hat der akkreditierte Diensteanbieter die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat darüber hinaus dafür zu sorgen, dass das De-Mail-Konto von einem anderen akkreditierten Diensteanbieter übernommen wird. Ferner hat er die betroffenen Nutzer über die Einstellung seiner Tätigkeit und die Übernahme des De-Mail-Kontos durch einen anderen akkreditierten Diensteanbieter zu benachrichtigen.

Die Übernahme eines De-Mail-Kontos durch einen anderen Diensteanbieter kann für beide Dienstanbieter zusammen mit Kosten in Höhe von 50.000 € bis 1 Mio. € verbunden sein. Die große Spanne ergibt sich daraus, dass beide Dienstanbieter die gleichen oder grundlegend unterschiedliche IT-Systeme und –Applikationen einsetzen können. Werden beispielsweise zwei Dienstanbieter von einem Provider auf einer gemeinsamen Plattform gehostet, so ist eine Übernahme problemlos und ohne große Kosten realisierbar.
Unter der Annahme von einer derartigen Übernahme pro Jahr ergeben sich durchschnittliche Kosten in Höhe von ca. 500.000 €.

Insgesamt ist für die akkreditierten Diensteanbieter mit folgenden jährlichen Bürokratiekosten zu rechnen – jeweils gemittelt über die ersten fünf Jahre:

- Nachweis Akkreditierungsvoraussetzungen und Akkreditierung (ohne Nachweis für die Deckungsvorsorge) 1,320 Mio. €
- Aufbewahrung der Dokumentation der Vertragsverhältnisse 0,162 Mio. €
- Auskunftserteilung über die Identität von Nutzern 0,540 Mio. €
- Übernahme De-Mail-Konto bei Einstellung der Tätigkeit 0,500 Mio. €

2,522 Mio. €

Darüber hinaus ergeben sich für die Diensteanbieter weitere jährliche Kosten – wiederum gemittelt über die ersten fünf Jahre:

- Deckungsvorsorge 1,080 Mio. €
- Zuverlässige Identitätsfeststellung (Erstregistrierung,) 18,512 Mio. €

19,592 Mio. €

Die jährlichen Gesamtkosten belaufen sich damit auf 22,114 Mio. €.

Informationspflichten und Kosten für Bürgerinnen und Bürger

Nach § 3 kann jede Person ein De-Mail-Konto beantragen. Zur zuverlässigen Identitätsfeststellung hat sie dem Diensteanbieter Nachweise vorzulegen. Dies kann durch Vorlage eines gültigen amtlichen Ausweises, z.B. bei einer Registrierungsstelle des Diensteanbieters oder durch Nutzung eines etablierten Identifizierungsverfahrens erfolgen. Zur Identitätsfeststellung kann auch der elektronische Identitätsnachweis im Sinne von § 18 des Personalausweisgesetzes genutzt werden. Als weitere Möglichkeit ist vorgesehen, dass mit Einwilligung der Person auch Daten verwendet werden können, die im Rahmen einer früheren zuverlässigen Identitätsfeststellung erhoben worden sind. Damit wird für Bürgerinnen und Bürger ein breites Spektrum an Möglichkeiten angeboten, um ein De-Mail-Konto zu eröffnen und damit die Einstiegshürde möglichst gering gehalten.

Die Eröffnung eines De-Mail-Kontos ist für die Bürgerinnen und Bürger in Abhängigkeit von der gewählten Identitätsfeststellung mit unterschiedlichem Zeitaufwand verbunden:

- Identitätsfeststellung beim Diensteanbieter oder Nutzung eines Identifizierungsverfahrens (mit persönlichem Erscheinen vor Ort) – ca. 40. Minuten
- Nutzung eines Identifizierungsverfahrens „an der Haustür“ – ca. 20 Minuten
- Nutzung elektronischer Identitätsnachweis im Sinne von § 18 des Personalausweisgesetzes – 10 Minuten
- Nutzung von bereits zuverlässig festgestellten Identitätsdaten – 10 Minuten

In den ersten Jahren ist von einer überwiegenden Nutzung der etablierten Identifizierungsverfahren auszugehen, so dass ein durchschnittlicher Zeitaufwand von 30 Minuten pro Kontoeröffnung zugrunde gelegt werden kann.

Nach fünf Jahren wird bereits etwa die Hälfte der Bevölkerung über den neuen Personalausweis verfügen und diesen in der Regel zur Kontoeröffnung einsetzen. Damit könnte sich der Zeitaufwand auf durchschnittlich ca. 20 Minuten reduzieren.

Ferner hat der akkreditierte Diensteanbieter nach § 9 Absatz 2 dem Nutzer eine Belehrung in Textform zu übermitteln, deren Kenntnisnahme dieser als Voraussetzung für die Freischaltung des De-Mail-Kontos ausdrücklich zu bestätigen hat. Da die Bestätigung der Kenntnisnahme auch elektronisch erfolgen kann, sind damit für die Bürgerinnen und Bürger keine Kosten verbunden.

Für die Kenntnisnahme der Belehrung und deren Bestätigung, die in der Regel elektronisch erfolgen wird, ist von einem Zeitlaufwand von durchschnittlich 10 Minuten auszugehen.

Damit ergibt sich durch die beiden neuen Informationspflichten für Bürgerinnen und Bürger ein zusätzlicher Zeitaufwand von 40 Minuten in den ersten fünf Jahren und 30 Minuten in den folgenden fünf Jahren.

Informationspflichten und Kosten für die Verwaltung

Für die Verwaltung, d.h. für die zuständige Behörde werden neue Informationspflichten im Rahmen der Akkreditierung von Diensteanbietern eingeführt.

Im Einzelnen:

- Nach § 17 können sich Diensteanbieter auf schriftlichen Antrag von der zuständigen Behörde akkreditieren lassen. Die Akkreditierung ist nach wesentlichen Veränderungen, spätestens jedoch nach drei Jahren zu wiederholen.
  Für die Maßnahmen zur Akkreditierung erhebt die zuständige Behörde Kosten (Gebühren und Auslagen).

- Falls beim Einstellen der Tätigkeit eines Diensteanbieters kein anderer Dienstanbieter die Dokumentation nach § 13 übernimmt, ist die zuständige Behörde nach § 11 Absatz 3 zur Übernahme verpflichtet. In diesem Fall erteilt die zuständige Behörde bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.

- Die Aufsicht der zuständigen Behörde bezieht sich nach § 20 auf die akkreditierten Diensteanbieter. Insbesondere kann die zuständige Behörde z. B. den Betrieb untersagen.
  Für die Maßnahmen im Rahmen der Aufsicht erhebt die zuständige Behörde Kosten (Gebühren und Auslagen).

- Nach § 22 hat die zuständige Behörde die Namen der akkreditierten Diensteanbieter und der ausländischen Diensteanbieter nach § 19 für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

V. Nutzenbetrachtungen

Das Gesetz verfolgt insbesondere das Ziel, die elektronische Kommunikation im Rechts- und Geschäftsverkehr voranzubringen. Dadurch wird sich der Anteil der mit hohen Porto-, Material- und Prozesskosten versehenen Papierpost deutlich reduzieren. Auf diesen Aspekt fokussieren die nachfolgenden Nutzenbetrachtungen. Einsparungen auf Basis der anderen

De-Mail-Dienste (Identitätsbestätigungsdienst und Dokumentenablage) und aufgrund einer generellen Verbesserung der heutigen elektronischen Kommunikationsformen bleiben unberücksichtigt.

In Deutschland werden pro Jahr ca. 17,5 Mrd. Briefsendungen im lizenzpflichtigen Bereich (gewerbsmäßige Beförderung von Briefsendungen bis 1000 g) verschickt. Der Anteil der Briefsendungen unter 50 g beträgt ca. 75 %. Die verbleibenden 25 % der Briefsendungen ab 50 g (bis 1000 g) werden im Weiteren nicht berücksichtigt, da es sich dabei zum großen Teil um Buch- und Katalogsendungen handelt, die nicht durch De-Mail-Nachrichten ersetzt werden können.

Den Nutzenbetrachtungen liegen demnach zunächst nur die ca. 13,125 Mrd. Briefsendungen < 50 g zu Grunde. Darüber hinaus wird angenommen, dass von diesen Briefsendungen nur 75 % grundsätzlich als elektronische Nachrichten durch den Postfach- und Versanddienst der De-Mail-Dienste versendet werden können, da 25 % aus unterschiedlichsten Gründen weiterhin als Papierpost verschickt werden sollen oder müssen. Damit sind ca. 9,844 Mrd. Briefe < 50 g pro Jahr grundsätzlich als De-Mail-Nachrichten versendbar.

Diese verteilen sich wiederum zu ca. 80 % auf die Wirtschaft und zu jeweils ca. 10 % auf öffentliche Verwaltung und Bürger.

Ferner wird der gegenwärtige Nutzungsgrad des Internets wie folgt berücksichtigt: Wirtschaft und Verwaltung mit jeweils 80 %, Bürgerinnen und Bürger mit 55 %. Diese Anteile reduzieren die Anzahl der grundsätzlich per De-Mail-Nachrichten versendbaren Briefe nochmals, woraus sich folgende Basiswerte ergeben:

- Wirtschaft 6,300 Mrd. Briefe
- Verwaltung 0,788 Mrd. Briefe
- Bürgerinnen und Bürger 0,541 Mrd. Briefe

Ferner wird angenommen, dass sich der Anteil der über die De-Mail-Dienste versendeten Nachrichten wie folgt entwickeln wird: 1. Jahr 2 %, 2. Jahr 5 %, 3. Jahr 10 %, 4. Jahr 15 % und 5. Jahr 20 % (jeweils bezogen auf die grundsätzlich als De-Mail-Nachrichten versendbaren Briefsendungen < 50 g).
Die Material- und Prozesskosten für den automatisierten Massenversand von Briefsendungen (z.B. Rechnungen) bewegen sich in einem unteren zweistelligen Cent-Bereich. Individuell erstellte Briefsendungen sind insbesondere aufgrund der dafür benötigten Arbeitszeit mit Prozesskosten für Erstellen, Drucken, Adressieren, Frankieren, Kuvertieren und Versenden im einstelligen Euro-Bereich verbunden. Aus diesem Grunde wird ein Einsparpotential für Wirtschaft und Verwaltung von durchschnittlich ca. 0,25 bis 0,50 € pro Briefsendung zugrunde gelegt.

Für Bürgerinnen und Bürger ergeben sich relevante Einsparungen bei den Kosten für Verbrauchsmaterial für Druck und Kuvertierung. Abhängig von der Seitenzahl pro Sendung ergibt sich Einsparpotential von 0,08 Euro bis 0,15 Euro pro Brief.

Ferner ist davon auszugehen, dass der Preis pro De-Mail-Nachricht unter den heute üblichen Portokosten im Papierpostbereich liegen wird und sich daraus weitere Einsparpotentiale ergeben. Die Höhe der Einsparungen lässt sich allerdings gegenwärtig noch nicht beziffern, da sich marktgerechte Preise für De-Mail-Nachrichten (De-Mail) erst im Wettbewerb bilden müssen. Daher bleibt dieses Einsparpotential in den folgenden Berechnungen zwar als Zahlenwert unberücksichtigt, sollte jedoch qualitativ immer in die Überlegungen einbezogen werden.

Auf die ersten fünf Jahre bezogen, ist unter diesen Annahmen von folgenden Einsparpotentialen (ohne Portokosten) auszugehen – alle Angaben gerundet auf Mio. €:

	Wirtschaft	**Verwaltung**	**Bürgerinnen und Bürger**
1. Jahr	30 Mio. - 60 Mio. €	3,75 Mio. € - 7,5 Mio. €	1,2 Mio. € - 2,25 Mio. €
2. Jahr	75 Mio. € - 150 Mio. €	9,375 Mio. € - 18,75 Mio. €	3 Mio. € - 5,625 Mio. €
3. Jahr	150 Mio. € - 300 Mio. €	18,75 Mio. € - 37,5 Mio. €	6 Mio. € - 11,25 Mio. €
4. Jahr	200 Mio. € - 400 Mio. €	25 Mio. € - 50 Mio. €	8 Mio. € - 15 Mio. €
5. Jahr	300 Mio. € - 600 Mio. €	37,5 Mio. € - 75 Mio. €	12 Mio. € - 22,5 Mio. €

Wenn wie bereits im 5. Jahr nur 8,71 % (20 % von 43,6 %) der gesamten Briefsendungen unter 50 g durch De-Mail-Nachrichten ersetzt werden, beträgt das jährliche Gesamt-Einsparungspotential in Deutschland für Wirtschaft, Verwaltung sowie Bürgerinnen und Bürger zusammen ca. 349,5 bis 697,5 Mio. Euro zzgl. der Portokosteneinsparungen.

VI. Auswirkungen von gleichstellungspolitischer Bedeutung

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1

Zum Abschnitt 1 (Allgemeine Vorschriften)

Zu § 1

Die Vorschrift nennt die Eigenschaften der De-Mail-Dienste im Sinne dieses Gesetzes. De-Mail-Dienste werden über eine Plattform für die elektronische Kommunikation angeboten. De-Mail-Dienste im Sinne dieses Gesetzes sollen sicheren elektronischen Rechts- und Geschäftsverkehr für jedermann – z. B. für Bürgerinnen und Bürger und Angehörige der Wirtschaft, Verwaltung oder Justiz ermöglichen und das Internet als Mittel für rechtsverbindliches und vertrauliches Handeln ausbauen. Das Angebot von De-Mail-Diensten ermöglicht die aufgezählten Dienste. Von den Diensten muss neben dem Verzeichnisdienst der Postfach- und Versanddienst angeboten werden. Akkreditierte Diensteanbieter müssen diese Dienste als Pflichtdienste anbieten, weil nur die Möglichkeit ihrer kombinierten Nutzung eine hohe Vertrauenswürdigkeit und Rechtssicherheit elektronischer Kommunikation bietet. Zusätzlich hinzutreten können der Identitätsbestätigungsdienst sowie der Dienst Dokumentenablage. Absatz 2 Satz 2 bestimmt den nach diesem Gesetz akkreditierten Diensteanbieter als Anbieter von De-Mail-Diensten... Diensteanbieter können natürliche oder juristische Personen sein. Die Nutzung von De-Mail-Diensten durch den einzelnen Nutzer erfolgt über ein De-Mail-Konto. Ein De-Mail-Konto kann jede Person (vgl. § 3 Absatz 1) eröffnen.

Zu § 2 (Zuständige Behörde)

Die Verwaltungskompetenz des Bundes stützt sich auf Artikel 87 Absatz 3 Satz 1 Grundgesetz. Um das erforderliche einheitliche Sicherheitsniveau zu gewährleisten, ist es erforderlich, die Aufgaben einer Bundesbehörde zu übertragen.
Das BSI verfügt über die erforderlichen Voraussetzungen für die Wahrnehmung der genannten Aufgaben. Unter verwaltungsökonomischen Gesichtspunkten ist die Übertragung der Aufgaben der Akkreditierung und der Aufsicht auf das BSI die beste Lösung. Bei Problemen hinsichtlich der Sicherheit eines der De-Mail-Dienste wird es sich in den meisten Fällen um komplexe IT-Sicherheitsfragen handeln, bei deren Lösung das BSI mit seiner Fachkompetenz ohnehin beteiligt wird. Die administrativen Tätigkeiten nehmen nur eine untergeordnete Rolle ein, während die fachliche Kompetenz im Vordergrund steht.

Zum Abschnitt 2 (Pflichtangebote und optionale Angebote des Diensteanbieters)

Die §§ 3 bis 8 enthalten Anforderungen an das Erbringen der Pflichtdienste und optionalen Angebote akkreditierter Diensteanbieter. Um ihrer Aufgabe als Dienstleister für eine Infrastruktur vertrauenswürdiger Dienstleistungen für den sicheren elektronischen Rechts- und Geschäftsverkehr gerecht werden zu können, bieten die akkreditierten Diensteanbieter in ihrem Zusammenwirken mehrere aufeinander abgestimmte Dienstleistungen zuverlässig an. Diese werden mit ihren Anforderungen an die Vertrauenswürdigkeit näher bestimmt.

Einen Antrag auf Akkreditierung werden vermutlich vor allem Dienstleister stellen, die bisher schon Postfach- und Versanddienste oder ähnliche Dienste anbieten. Diese bestehenden Angebote bleiben durch die Akkreditierung unberührt. Dadurch kann ein Diensteanbieter einen den §§ 3 bis 8 entsprechenden Dienst als akkreditierter Diensteanbieter und zugleich einen funktional vergleichbaren Dienst mit geringeren Vertrauenswürdigkeitsanforderungen als nicht akkreditierter Diensteanbieter anbieten. Auch können akkreditierte Diensteanbieter weitere Dienste als die in §§ 3 bis 8 genannten anbieten. Für die Vertrauenswürdigkeit der Dienste, die er als akkreditierter Diensteanbieter anbietet, und für die Markttransparenz ist

daher eine eindeutige Unterscheidbarkeit dieser Dienste und ihrer Nutzung von anderen Diensten erforderlich.

Zu § 3 (Eröffnung eines De-Mail-Kontos)

Ein De-Mail-Konto bietet die Nutzung verschiedener Dienste an. Das De-Mail-Konto eröffnet daher die Möglichkeit, die im Folgenden geregelten Dienste zu nutzen.
Soweit das Gesetz keine speziellen Anforderungen stellt, bleibt das Erbringen und die Inanspruchnahme der im Gesetz genannten Dienstleistungen vertraglichen Vereinbarungen zwischen den Beteiligten vorbehalten. Bei der Vertragsabwicklung sind die Belange des Verbraucherschutzes zu beachten. So sollten z.B. bei einer Internetbasierten Vertragsanbahnung seitens des akkreditierten Diensteanbieters
- freiwillige und Pflichteingabefelder deutlich als solche gekennzeichnet werden;
- Pflichteingabefelder auf die zur Durchführung des Vertrags erforderlichen Angaben beschränkt werden;
- die letzte Schaltfläche zum Absenden des Antrages eindeutig als solche gekennzeichnet sein, z.B. durch die Beschriftung „Antrag absenden“;
- zu jeder abgeschlossenen Beantragung dem Antragsteller als Nachweis des Eingangs in verkehrsüblicher Zeit eine Empfangsbestätigung zugesendet werden. Die Empfangsbestätigung muss ausdruckbar sein und zusätzlich per E-Mail versandt werden, sofern der Antragsteller eine E-Mail-Adresse angegeben hat.

Ist ein Nutzer nicht unbeschränkt geschäftsfähig, so richtet sich die Möglichkeit des Erwerbs und der Nutzung von De-Mail-Konten nach den Bestimmungen des Bürgerlichen Gesetzbuches zur Geschäftsfähigkeit.

Mit der Voraussetzung eines Mindestalters von 16 Jahren für die Eröffnung eines De-Mail-Kontos soll den Belangen des Jugendschutzes nachgekommen werden; außerdem wird somit ein Gleichklang zu § 10 Absatz 3 des Personalausweisgesetzes vom 18. Juni 2009 (BGBl. I, S. 1346) hergestellt, wonach die Einschaltung des elektronische Identitätsnachweises ein Mindestalter von 16 Jahren erfordert.

Ein Kontrahierungszwang ist nicht vorgesehen, da davon ausgegangen werden kann, dass der Markt jedem Interessenten die Möglichkeit eröffnen wird, bei einem Diensteanbieter ein De-Mail-Konto zu erlangen.

Die zuverlässige Identifizierung des zukünftigen Nutzers (Antragsteller) ist eine wesentliche Voraussetzung dafür, dass De-Mail-Dienste ihre Aufgabe als sichere Vertrauensanker im Kommunikationsraum Internet erfüllen.
Zur Feststellung der Identität des Antragstellers erhebt der akkreditierte Diensteanbieter die in Absatz 2 Satz 2 genannten Angaben. Die vorgesehene Feststellung des Namens bei natürlichen Personen umfasst den Nachnamen und mindestens einen Vornamen.
Zur Überprüfung der Identität des Antragstellers hat sich der akkreditierte Diensteanbieter anhand der in Absatz 3 genannten Dokumente zu vergewissern, dass die erhobenen Angaben zutreffend sind. Die Regelung orientiert sich an § 4 Geldwäschegesetz vom 13. August 2008 (BGBl. I S. 1690); auf die Begründung dieser Regelung (Drs. 16/9038, S. 36) wird verwiesen. Eine medienbruchfreie Identitätsfeststellung mit Hilfe des elektronischen Identitätsnachweises im Sinne des § 18 Personalausweisgesetz ist ebenfalls zulässig. Auf die Begründung dieser Regelung (BT-Drs. 16/10489, S. 40ff) wird verwiesen.
Anhaltspunkte dazu, welche weiteren Dokumente zur Identitätsüberprüfung geeignet sind, können sich aus der nach § 4 Absatz 4 Satz 2 des Geldwäschegesetzes zu erlassenden Verordnung ergeben.

Absatz 3 Satz 2 dient der Klarstellung, dass der Diensteanbieter zu einem früheren Zeitpunkt erhobene Daten des Nutzers unter Beachtung seiner datenschutzrechtlichen Belange zum Zweck der Identifizierung nutzen darf. Voraussetzung dafür ist, dass die Identifizierung die

Anforderungen des Absatzes 2 Satz 1 erfüllt, die Daten aktuell sind und der Antragsteller mit der Verwendung dieser Daten für diesen Zweck einverstanden ist. Unter diesen engen Voraussetzungen können daher beispielsweise auch beim Diensteanbieter vorhandene Kundendaten, die dieser bei Aufnahme einer anderen Geschäftsbeziehung mit dem Nutzer erhoben hatte, für die Identifizierung verwendet werden. Als zu einem früheren Zeitpunkt durch den Diensteanbieter erhobene Daten gelten auch die Daten, die ein nach § 18 Absatz 4 beauftragter Dritter erhoben hat.

Die Regelung ist bußgeldbewehrt (vgl. § 23 Absatz 1 Nr. 1).

Absatz 4 beschreibt den Vorgang der Freischaltung eines De-Mail-Kontos durch den akkreditierten Diensteanbieter.

Absatz 5 orientiert sich an § 3 Absatz 1 Nummer 4 des Geldwäschegesetzes, der eine ähnlich gelagerte Sorgfaltspflicht zur Überwachung der fortdauernden Stimmigkeit von Daten enthält. Zweck der Regelung ist die Erhaltung der Aktualität der Identifikationsdaten des Nutzers. Die akkreditierten De-Mail-Diensteanbieter haben Maßnahmen zu ergreifen, um sicherzustellen, dass die Identifikationsdaten ihrer Nutzer auf einem aktuellen Stand sind und der Wahrheit entsprechen. Dies umfasst zum einen die Verpflichtung, die Daten aktiv zu überprüfen, wenn Anlass für die Vermutung besteht, dass die Identitätsdaten eines Nutzers nicht oder nicht mehr zutreffen. Zum anderen kann der Anbieter seiner Sorgfaltspflicht nachkommen, indem er die Nutzer vertraglich zur Aktualisierung seiner Daten verpflichtet, sobald diese sich ändern.

Zu § 4 (Sichere Anmeldung zu einem De-Mail-Konto)

Die Vorschrift regelt eine wesentliche Voraussetzung für die Vertrauenswürdigkeit sämtlicher De-Mail-Dienste. Während der in § 3 beschriebene Vorgang der Eröffnung eines De-Mail-Kontos einmal erfolgt, findet die Anmeldung nach § 4 jedes Mal statt, wenn man seine De-Mail-Dienste nutzen möchte; sie entspricht dem Vorgang des „Einloggens“ bei einem „normalen“ E-Mail-Konto, stellt hier jedoch eine qualifizierte Art des „Einloggens“ dar. Vor jeder Nutzung der De-Mail-Dienste ist das Anmelden an dem individuellen De-Mail-Konto erforderlich. Die Nutzung bestimmter Dienste erfordert die Wahl einer sicheren Anmeldung. Auf der sicheren Anmeldung beruht das Vertrauen in die Authentizität der über den De-Mail-Dienst ausgeführten Handlungen. Zur besseren Nutzbarkeit ist jedoch auch eine Anmeldung zum De-Mail-Konto mit Benutzernamen und Passwort möglich, ohne dass also eine sichere Anmeldung im Sinne von Absatz 1 Satz 1 vorliegt.

Hintergrund der Anforderung an den akkreditierten Diensteanbieter, eine sichere, z.B. durch Besitz und Wissen geschützte Anmeldung anzubieten, ist die bisherige Rechtsprechung zur Annahme eines Anscheinsbeweises bei Zugangssicherungen mittels Benutzername und Passwort. Soweit im Einzelfall zwischen den Kommunikationspartnern Streit über rechtlich oder wirtschaftlich erhebliche Handlungen entsteht, die über den De-Mail-Dienstl abgewickelt wurden, ist zu erwarten, dass sich der Nutzer eines De-Mail-Dienstes auch darauf berufen wird, dass sich ein Dritter unbefugt unter seinem Namen angemeldet und gehandelt hat. Die Vornahme einer Handlung unter einem bestimmten De-Mail-Konto stellt aufgrund der vielfältigen Manipulationsmöglichkeiten im Internet ohne die Berücksichtigung weiterer Umstände regelmäßig keinen Beweis dafür dar, dass die Handlung auch tatsächlich von dem Nutzer des De-Mail-Kontos vorgenommen wurde. Bestreitet der Nutzer die Handlung, so dürfte ein gegenteiliger Beweis durch den Kommunikationspartner in der Regel schwierig oder gar nicht zu führen sein. Die Rechtsprechung hat einen Anscheinsbeweis für die rechtmäßige Anmeldung bei einer Sicherung durch Benutzernamen und Passwort regelmäßig abgelehnt und eine Sicherung durch Besitz und Wissen gefordert, um einen Anscheinsbeweis für die Authentizität der Handlung anzunehmen. Um Rechtssicherheit für den elektronischen Rechts- und Geschäftsverkehr durch die Nutzung von De-Mail-Diensten zu schaffen, muss die Anmeldung zu diesen, soweit sie der Vornahme beweisrelevanter

Handlungen dient, beweissicher erfolgen. Der akkreditierte Diensteanbieter hat dies dem Nutzer als eine Grundeigenschaft des De-Mail-Dienstes zu ermöglichen.

Den heutigen Sicherheitsanforderungen entspricht die Verwendung von zwei voneinander unabhängigen Sicherungsmitteln. Die technikneutrale Formulierung belässt dem De-Mail-Diensteanbieter einen Spielraum, der die Anpassung des Anmeldeverfahrens an den technischen Fortschritt ermöglicht. Sofern der De-Mail-Diensteanbieter für die sichere Anmeldung Geheimnisse benutzt, muss er sicherstellen, dass diese einmalig sind und geheim gehalten werden können. Die Einmaligkeit und Geheimhaltung der verwendeten Geheimnisse muss auch durch die Form der Übergabe der Sicherungsmittel gewährleistet sein.

Eine gesonderte Regelung der Anmeldung juristischer Personen kann an dieser Stelle unterbleiben. Die Verteilung der Adressen eines De-Mail-Dienstes, die Regelung der Nutzung durch mehrere Nutzer im Namen einer juristischen Person und die Sicherung der Zuordnung einzelner Handlungen betrifft nicht den akkreditierten Diensteanbieter. Auch die Haftung der juristischen Person ist durch allgemeine Grundsätze ausreichend geregelt. Sie erhält eine sichere Anmeldungsmöglichkeit, alle weiteren Regelungen für den inneren Ablauf bleiben ihr selbst überlassen.

Die Regelung des Absatzes 1 Satz 2 ist bußgeldbewehrt vgl. (§ 23 Absatz 1 Nr. 2).

In Absatz 2 ist geregelt, dass dem Nutzer mindestens zwei Verfahren zur sicheren Anmeldung zur Verfügung gestellt werden müssen, wobei im Rahmen eines der beiden Verfahren zwingend der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes genutzt werden können muss,. Alternativ ist mindestens ein weiteres Verfahren vorzusehen; damit ist sichergestellt, dass der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes nicht Voraussetzung für die Nutzung eines De-Mail-Kontos ist. Da sich die De-Mail-Infrastruktur und Funktionen des neuen Personalausweises aber sinnvoll ergänzen, soll der Nutzer, wenn er möchte, den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes nutzen können.

Zu § 5 (Postfach- und Versanddienst)

Für die sichere Kommunikation im Internet ist ein sicherer Postfach- und Versanddienst von entscheidender Bedeutung. Er ermöglicht eine Kommunikation zwischen vertrauenswürdigen Sendern und Empfängern und den Nachweis der Übermittlung bestimmter Nachrichten zu einem bestimmten Zeitpunkt. Der akkreditierte Diensteanbieter ist verpflichtet, diesen Dienst anzubieten. Mit der Nutzungsmöglichkeit des Postfach- und Versanddienstes ist das Postfach des Nutzers als Empfangsbereich in der Weise zu werten, als durch das Einlegen einer Nachricht in das Postfach durch den akkreditierten Diensteanbieter diese Nachricht in der Regel als im Sinne von § 130 BGB als zugegangen gilt. In diesem Moment ist grundsätzlich die Kenntnisnahme durch den Empfänger möglich und nach der Verkehrsanschauung auch zu erwarten (vgl. Palandt, 68. Auflage 2009, § 130 Rn. 5).

Zu Absatz 1

Die Vertrauenswürdigkeit des Postfach- und Versanddiensts wird zum einen dadurch gewährleistet, dass der berechtigte Nutzer bei der Zuteilung der De-Mail-Adresse zuverlässig identifiziert worden ist, so dass die Sender und Empfänger sich darauf verlassen können, dass der in der Nachricht angegebene Sender oder Empfänger mit diesem Nutzer identisch ist. Zum anderen beruht die Vertrauenswürdigkeit darauf, dass der Sender und der Empfänger für den Zugang zu diesem Dienst sich jeweils, wenn und gegebenenfalls wie dem Kommunikationspartner angegeben oder von diesem gefordert, an ihrem De-Mail-Konto sicher angemeldet haben. Schließlich beruht die Vertrauenswürdigkeit darauf, dass die Nachricht vom Diensteanbieter verschlüsselt übermittelt wird, so dass sie auf dem Transportweg weder ausgespäht noch spurenlos verändert werden kann.

Dies schließt Ende-zu-Ende-Sicherheitsmaßnahmen der Nutzer, die für bestimmte Inhalte oder die Kommunikation bestimmter Berufsvertreter erforderlich sind, wie Inhaltsverschlüsselung oder Signaturen nicht aus. Diese Sicherungsmaßnahmen werden vom sicheren Postfach- und Versanddienst unterstützt.

Die Sätze 2 und 3 enthalten Anforderungen an das Format der De-Mail-Adresse:

Nach Satz 3 kann/muss im Domänenteil („hinter dem @“) der Adresse eine einheitliche Kennzeichnung vorgesehen werden. Diese ist bei allen De-Mail-Adressen (natürlichen wie juristischen Personen, Personengesellschaften und öffentlichen Stellen) gleich. An dieser Kennzeichnung wäre die De-Mail-Adresse als solche erkennbar. Nur akkreditierte Diensteanbieter wären berechtigt und verpflichtet, an ihre Nutzer De-Mail-Adressen mit der einheitlichen Kennzeichnung zu vergeben. Bei der einheitlichen Kennzeichnung kann es sich um eine Top-Level-Domain oder um eine Sublevel-Domain handeln.

Nach Satz 2 Nummer 1 wird dem Nutzer, soweit es sich um eine natürliche Person (zur Unterscheidung vgl. § 3 Absatz 2 und 3) handelt, vom akkreditierten Diensteanbieter genau eine Hauptadresse (im Gegensatz zu Pseudonymadressen, siehe Absatz 2) zugewiesen, die im lokalen Teil der Adresse („vor dem @“) dessen Nachnamen und auf Wunsch des Nutzers dessen Vorname oder Vornamen oder Teile des oder der Vornamen enthalten muss und gegebenenfalls eine Nummer, wenn mehrere Nutzer dieselbe Kombination von Vor- und Nachnamen wünschen.

Nach Satz 2 Nummer 2 muss der akkreditierte Diensteanbieter dem Nutzer, soweit es sich um eine juristische Person, Personengesellschaft oder öffentliche Stelle handelt, eine De-Mail-Adresse anbieten, die im Domänenteil („hinter dem @“) eine vom Nutzer beantragte Bezeichnung („jurPerson-Nutzer-Domain“) enthält. Diese Bezeichnung muss in direktem Bezug zu Firma, Namen oder Bezeichnung des betreffenden Nutzers stehen. Außerdem müssen – soweit der Nutzer (als juristische Person, Personengesellschaft oder öffentliche Stelle) dies verlangt – weitere Subdomains eingerichtet werden können, welche der Kennzeichnung von Unterbereichen des entsprechenden Nutzers dienen (z.B. Bezeichnungen von Abteilungen, Niederlassungen, Standorten); bei diesen Subdomains handelt es sich jeweils um eine Untergliederung der jurPerson-Nutzer-Domain („jurPerson-Nutzer-Domain-Untergliederung“). Diese sind optionaler Bestandteil der De-Mail-Adresse. Ebenso ist bei den De-Mail-Adressen der juristischen Personen etc. der Bestandteil der Domain des akkreditierten Diensteanbieters optional.

Zu Absatz 2

Die Nutzung von De-Mail-Diensten ohne pseudonyme De-Mail-Adressen würde das Erstellen von Persönlichkeitsprofilen (z.B. bezüglich des Kaufverhaltens von Personen) ermöglichen. Durch die Verwendung von pseudonymen De-Mail-Adressen wird die Zuordnung der Daten zu einer Person verhindert oder zumindest erschwert. Es steht im Belieben des akkreditierten Diensteanbieters, Pseudonym-Adressen anzubieten.

Pseudonyme sind nach Satz 2 als solche kenntlich zu machen, um Verwechslungen mit tatsächlichen Personen zu vermeiden und einem entsprechenden Identitätsmissbrauch vorzubeugen. Die Kennzeichnung erfolgt in einer pseudonymen De-Mail-Adresse durch die Buchstabenkombination „pn_“.

Nicht als Pseudonym kenntlich gemacht werden müssen der Name einer juristischen Person und einer ihrer Funktionseinheiten, da hier eine Verwechslungsgefahr mit einer natürlichen Person ausgeschlossen ist.

Zu Absatz 3

Die Sicherung der Vertraulichkeit, der Integrität und der Authentizität ist die Eigenschaft des Postfach- und Versanddienstes, die diesen von vergleichbaren Diensten unterscheidet. Aus diesem Grund ist sie ein Definitionsmerkmal dieses De-Mail-Dienstes. Die Sicherung erfolgt

Kommentar [KJ2]: Dieser Satz wird im Rahmen der weiteren Abstimmung mit Ressorts, Ländern und Verbänden höchstwahrscheinlich zu kontroversen Diskussionen führen, da hier aus verschiedenen Gründen unterschiedliche Auffassungen bestehen, die dem BMI bereits bekannt sind. Im Verlauf der Ressorts-, Länder- und Verbändebeteiligung sollen weitere Argumente gesammelt werden, auf deren Basis besser bewertet werden kann, ob eine einheitliche Kennzeichnung im Domänenteil vorgesehen werden kann oder muss oder ob hierauf nicht auch verzichtet werden kann. Der Satz ist als ein erster Textvorschlag seitens des federführenden Ressorts BMI anzusehen, eine Entscheidung z.B. dahingehend, ob dies eine „Kann“ oder eine „Muss“-Regelung ist, soll damit noch nicht verbunden sein.

Kommentar [KJ3]: Die Hauptadresse einer natürlichen Person könnte also regelmäßig nach folgendem Schema aufgebaut sein (Mit „< >“ gekennzeichnete Bestandteile sind verpflichtend Bestandteil der De-Mail-Adresse; mit „[ ]“ gekennzeichnete Bestandteile sind optional):
[Teil des oder der Vorname(n).]<Nachname>[.Nummer]@<Domain des akkreditierten Diensteanbieters>.[einheitliche Kennzeichnung], ein Beispiel: hermann-gustav.mueller.123@mein-provider.einheitliche-Kennzeichnung.

Kommentar [KJ4]: Die Adresse einer juristischen Person, Personengesellschaft oder öffentlichen Stelle könnte also regelmäßig wie folgt lauten (Mit „< >“ gekennzeichnete Bestandteile sind verpflichtend Bestandteil der De-Mail-Adresse; mit „[ ]“ gekennzeichnete Bestandteile sind optional):
<lokaler Teil – frei wählbar>@[jurPerson-Nutzer-Domain-Untergliederung.]<jurPerson-Nutzer-Domain>[.<Domain des akkreditierten Diensteanbieters>].[<einheitliche Kennzeichnung], mehrere Beispiele:

-hans.mueller@dachdecker-mueller.einheitliche-Kennzeichnung;
-einkauf@dachdecker-mueller.einheitliche-Kennzeichnung;
-hans.mueller@verwaltung.dachdecker-mueller.einheitliche-Kennzeichnung;
-hans.mueller@dachdecker-mueller.mein-provider.einheitliche-Kennzeichnung

Kommentar [KJ5]: Die pseudonyme De-Mail-Adresse könnte also regelmäßig nach folgendem Schema aufgebaut sein (Mit „< >“ gekennzeichnete Bestandteile sind verpflichtend Bestandteil der De-Mail-Adresse; mit „[ ]“ gekennzeichnete Bestandteile sind optional):
<pn_>.<Bezeichnung nach Wahl des Nutzers>@<Domain des akkreditierten Diensteanbieters>.[einheitliche Kennzeichnung], ein Beispiel: pn_bellaerika@mein-provider.einheitliche-Kennzeichnung.

durch eine Verschlüsselung des Nachrichteninhaltes auf dem Transport zwischen den akkreditierten Diensteanbietern und durch die Sicherung des Zugangs zu den De-Mail-Diensten.

Zu Absatz 4

Je nach den Bedürfnissen oder Obliegenheiten des Senders und der Vertraulichkeit des Nachrichteninhalts kann für den Sender der Bedarf entstehen sicherzugehen, dass tatsächlich nur der adressierte Empfänger Zugriff auf den Nachrichteninhalt erhält. Diesem Bedarf, der etwa bei der Übermittlung von vertraulichen Daten oder für Sender mit besonderen Verschwiegenheitspflichten bestehen kann, wird durch die Möglichkeit Rechnung getragen, eine sichere Anmeldung des Nachrichtenempfängers zu fordern. Der Empfänger kann die Nachricht erst nach der sicheren Anmeldung einsehen. Verfügt der Empfänger nicht über die Möglichkeit einer sicheren Anmeldung, ist ein Zugang der Nachricht nicht möglich. In diesem Fall hat der Diensteanbieter des Empfängers die Nachricht mit einer entsprechenden Mitteilung an den Absender zurückzusenden, ohne sie in das Postfach des Empfängers zu übermitteln. Die Funktionen des Postfach- und Versanddienstes zu ermöglichen, gehört zu den gemeinschaftlich zu erfüllenden Pflichten der akkreditierten Diensteanbieter.

Zu Absatz 5

Der Empfänger einer über den Versanddienst versandten Nachricht erhält auf Verlangen des Senders eine beweissichere Bestätigung über dessen sichere Anmeldung. Der Sender soll bei jeder zu versendenden Nachricht erneut die Möglichkeit haben, zu entscheiden, ob die Bestätigung erzeugt wird. Die Beweissicherheit der Bestätigung kann etwa durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur des akkreditierten Diensteanbieters über diese Bestätigung gewährleistet werden. Durch diese Bestätigung erhält der Empfänger der elektronischen Nachricht ein belastbares Beweismittel. Eine aus Datenschutzgründen bedenkliche Speicherung der Zugriffe jeder einzelnen Anmeldung kann und wird daher unterbleiben.

Zu Absatz 6

Um auch im Internet ohne Beweisverlust förmliche Zustellungen durchführen zu können, werden die akkreditierten Diensteanbieter verpflichtet, daran mitzuwirken und die erforderlichen Bestätigungen auszustellen. Damit den von einem Diensteanbieter ausgestellten elektronischen Abholbestätigungen nach § 371a Absatz 2 Satz 1 in Verbindung mit § 418 der Zivilprozessordnung der Beweiswert einer öffentlichen Urkunde zukommt, muss der akkreditierte Diensteanbieter mit Hoheitsbefugnissen ausgestattet sein und ist in diesem Umfang beliehener Unternehmer. Im Interesse der Rechtssicherheit ist es erforderlich, dass jeder akkreditierte Diensteanbieter mit Wirksamwerden der Akkreditierung auch beliehen ist, ohne dass es eines gesonderten Beleihungsverfahrens bedarf.

Die Vorschrift korrespondiert mit der durch Artikel 2 eingeführten neuen Vorschrift des § 174 Absatz 3 Satz 4 der Zivilprozessordnung und der durch Artikel 3 eingeführten neuen Regelungen des Verwaltungszustellungsgesetzes. Die in Satz 1 in Bezug genommenen „Vorschriften der Prozessordnungen“ betreffen nur solche, welche Regelungen für die Zustellung über De-Mail-Dienste enthalten; eine allgemeine prozessrechtliche Zulässigkeit der Zustellung über De-Mail-Dienste wird damit nicht normiert.

Zu Absatz 7

Um dem Nutzer auch im Internet ohne Beweisverlust den Nachweis eines ordnungsgemäßen Versands einer Nachricht zu ermöglichen, wird der akkreditierte Diensteanbieter des Senders verpflichtet, auf dessen Antrag Versandbestätigungen auszustellen. Ein solcher Nachweis kann erforderlich sein, um etwa ein Versäumnis der Diensteanbieter oder die Voraussetzungen einer Wiedereinsetzung in den vorigen Stand nachweisen zu können. Die Versandbestätigung sollte dabei, um ihre Funktion zu erfüllen, die De-Mail-Adresse, an die zugestellt werden soll, das Datum und die Uhrzeit des Ausgangs der Nachricht aus dem De-Mail-Postfach des Senders, den Namen und Vornamen oder die

Firma des akkreditierten Diensteanbieters, der die Versandbestätigung erzeugt, sowie die Prüfsumme der Nachricht enthalten. Hierbei wird es sich üblicherweise um einen Hash-Wert handeln. Auf diese Weise wird der Sender der Nachricht in die Lage versetzt, auch zu beweisen, dass er den Inhalt der Nachricht tatsächlich versandt hat. Darüber hinaus können weitere Informationen in der Versandbestätigung enthalten sein. Darüber hinaus wird die Versandbestätigung mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen, um den mit der Versandbestätigung verbundenen Beweiszweck erfüllen zu können.

Zu Absatz 8

Damit der Rechts- und Geschäftsverkehr Nachrichten mit vertrauenswürdigen Nachweisen elektronisch übermitteln kann, bieten die Diensteanbieter im Zusammenwirken eine elektronische Zugangsbestätigung an. Der Diensteanbieter des Empfängers bestätigt in dieser auf Antrag des Senders, wann er welche Nachricht im De-Mail-Postfach des Empfängers abgelegt hat. Nach derzeitigem Stand der Technik signiert er hierfür die Prüfsumme der Nachricht und die Zeitangabe. Der akkreditierte Diensteanbieter hat dabei sicherzustellen, dass die Zeit an seinen Rechnern nicht manipuliert werden kann und regelmäßig überprüft wird. Die Möglichkeit der Kenntnisnahme einer auf diese Weise zugestellten Nachricht durch den Empfänger wird dadurch gewährleistet, dass der Empfänger, soweit er an seinem De-Mail-Konto nicht sicher im Sinne des § 4 angemeldet ist – also z.B. nur mittels Benutzername/Passwort – diese Nachricht 90 Tage lang nicht löschen kann.

Der Mindestinhalt der elektronischen Zugangsbestätigung richtet sich nach den Sätzen 4 und 5. Danach muss die Zugangsbestätigung auch die Prüfsumme der Nachricht enthalten. Hierbei wird es sich üblicherweise um einen Hash-Wert handeln. Auf diese Weise wird der Sender der Nachricht in die Lage versetzt, zu beweisen, dass auch der Inhalt der Nachricht, so wie er versandt wurde, zugegangen ist.

Der akkreditierte Diensteanbieter hat die Zugangsbestätigung zur Sicherung ihrer Authentizität und Integrität mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Auf diese Weise kann mithilfe der Zugangsbestätigung der Zugang der in den versendeten Nachrichten enthaltenen Willenserklärungen langfristig nachgewiesen werden.

Die dauerhafte Überprüfbarkeit bestimmt sich nach dem Stand der Technik. Derzeit heißt dies: Die qualifizierte elektronische Signatur und das ihr zugrunde liegende qualifizierte Zertifikat sind dauerhaft überprüfbar, wenn der Zertifizierungsdiensteanbieter sicherstellt, dass die von ihm ausgestellten Zertifikate an dem Zeitpunkt der Bestätigung des Erhalts einer sicheren Signaturerstellungseinheit durch den Signaturschlüssel-Inhaber für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikats endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Absatz 1 Satz 3 des Signaturgesetzes geführt werden. Der Zertifizierungsdiensteanbieter hat die Dokumentation im Sinn des § 10 des Signaturgesetzes und des § 8 der Signaturverordnung mindestens für diesen Zeitraum aufzubewahren. Signaturen nach § 15 Absatz 1 des Signaturgesetzes erfüllen diese Anforderungen

Zu Absatz 9

Zusätzlich zum Angebot der Zugangsbestätigung des Absatzes 8 bieten die Diensteanbieter im Zusammenwirken eine elektronische Abholbestätigung an. Diese ist jedoch nur von öffentlichen Stellen im Rahmen ihrer Berechtigung, förmlich zuzustellen, einsetzbar. Die Berechtigung, förmlich zu zustellen, ergibt sich immer aus einem Gesetz (z. B. § 1 Verwaltungszustellungsgesetz). Sender einer Nachricht, für welche eine Abholbestätigung verlangt wird, ist also immer eine öffentliche Stelle. Empfänger einer solchen Nachricht immer jemand, dem förmlich zugestellt wird. Der Empfänger wird darüber unterrichtet, dass es sich um eine förmliche Zustellung handelt. Der Diensteanbieter des Empfängers bestätigt in dieser Abholbestätigung auf Antrag der sendenden öffentlichen Stelle, wann er welche Nachricht im De-Mail-Postfach des Empfängers abgelegt hat und zusätzlich, wann der

Empfänger sich an seinem De-Mail-Konto im Sinne des § 4 angemeldet („eingeloggt“) hat. Nach derzeitigem Stand der Technik signiert er hierfür die Prüfsumme der Nachricht und die beiden Zeitangaben. Der akkreditierte Diensteanbieter hat dabei sicherzustellen, dass die Zeit an seinen Rechnern nicht manipuliert werden kann und regelmäßig überprüft wird. Hier wie bei der Zugangsbestätigung nach Absatz 8 gilt, dass die Möglichkeit der Kenntnisnahme einer auf diese Weise zugestellten Nachricht durch den Empfänger dadurch gewährleistet wird, dass der Empfänger, soweit er an seinem De-Mail-Konto nicht sicher im Sinne des § 4 angemeldet ist – also z.B. nur mittels Benutzername/Passwort – diese Nachricht 90 Tage lang nicht löschen kann.

Der Mindestinhalt der elektronischen Abholbestätigung richtet sich nach den Sätzen 4 und 5. Danach muss die Abholbestätigung auch die Prüfsumme der Nachricht enthalten. Hierbei wird es sich üblicherweise um einen Hash-Wert handeln. Auf diese Weise wird der Sender der Nachricht in die Lage versetzt, zu beweisen, dass auch der Inhalt der Nachricht, so wie er versandt wurde, zugegangen ist.

Der akkreditierte Diensteanbieter hat die Abholbestätigung zur Sicherung ihrer Authentizität und Integrität mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Auf diese Weise kann mithilfe der Abholbestätigung der Zugang der in den versendeten Nachrichten enthaltenen Willenserklärungen und zusätzlich der Zeitpunkt, zu welchem der Empfänger sich an seinem De-Mail-Konto angemeldet hat, langfristig nachgewiesen werden.

Die dauerhafte Überprüfbarkeit bestimmt sich nach dem Stand der Technik. Derzeit heißt dies: Die qualifizierte elektronische Signatur und das ihr zugrunde liegende qualifizierte Zertifikat sind dauerhaft überprüfbar, wenn der Zertifizierungsdiensteanbieter sicherstellt, dass die von ihm ausgestellten Zertifikate an dem Zeitpunkt der Bestätigung des Erhalts einer sicheren Signaturerstellungseinheit durch den Signaturschlüssel-Inhaber für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikats endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Absatz 1 Satz 3 des Signaturgesetzes geführt werden. Der Zertifizierungsdiensteanbieter hat die Dokumentation im Sinn des § 10 des Signaturgesetzes und des § 8 der Signaturverordnung mindestens für diesen Zeitraum aufzubewahren. Signaturen nach § 15 Absatz 1 des Signaturgesetzes erfüllen diese Anforderungen.

Zu Absatz 10

Zweck der Regelung ist es, den Zugang einer Nachricht sicherzustellen, indem die Löschung einer Nachricht, deren Zugang nach Absatz 8 oder Abholung nach Absatz 9 bestätigt wurde, unter Verwendung einer Zugangsstufe unterhalb der sicheren Anmeldung nach § 4 erschwert wird. Diese Maßnahme ist erforderlich um zu verhindern, dass zugegangene Nachrichten unter Umgehung der sicheren Anmeldung durch Dritte gelöscht werden können, bevor der Nutzer die Nachricht zur Kenntnis nehmen kann. Im Übrigen wird auf die Begründung zu Absatz 8 und 9 verwiesen.

Zu Absatz 11

Zweck der Regelung ist es, eine Funktion anzubieten, mit welcher ein Nutzer z.B. bei vorübergehender Abwesenheit, in welcher er sein De-Mail-Konto nicht nutzen kann, gewährleistet, dass ein von ihm gewählter Dritter Kenntnis von an ihn gerichtete Nachrichten erhält. Der Dritte kann dann soweit erforderlich den Nutzer darüber unterrichten, dass er – der Nutzer – eine wichtige De-Mail erhalten hat. Diese Funktion entspricht etwa der Möglichkeit in der realen Welt, dass man dem Nachbarn seinen Briefkastenschlüssel für die Zeit seines Urlaubs gibt und diesen bittet, den Briefkasten für ihn zu leeren und ihn gegebenenfalls über wichtige Nachrichten zu informieren.

Zu § 6 (Identitätsbestätigungsdienst)

Ob der Diensteanbieter den Identitätsbestätigungsdienst anbietet, steht in seinem Belieben.

Zu Absatz 1

Der Identitätsbestätigungsdienst eröffnet dem Nutzer die Möglichkeit, die bei ihm nach § 3 hinterlegten Identitätsdaten für eine sichere Identitätsbestätigung Dritten gegenüber zu nutzen. Durch die beweissichere Bestätigung der sicheren Anmeldung nach § 5 Absatz 5 kann die empfangene Authentisierung als Beweismittel genutzt werden.

Zu Absatz 2

Die Regelung soll die Integrität der Identitätsdaten und damit das notwendige Vertrauen in den Identitätsbestätigungsdienst sicherstellen. Dies erfordert vor allem wiederholte interne Kontrollen (z.B. stichprobenartiger Vergleich der Daten mit den jeweiligen Anträgen). Da speziell technisch bedingte Verfälschungen von Daten nicht ausgeschlossen werden können, müssen diese zumindest zwangsläufig bemerkt werden (z.B. durch Anwendung elektronischer Signaturen und Zeitstempel bei der Datenspeicherung und -übermittlung).

Zu Absatz 3

Absatz 3 stellt die Entscheidung, ob in den dort genannten Fällen eine Sperrung eines Identitätsdatums geboten ist, in das pflichtgemäße Ermessen der zuständigen Behörde. Der Vorschrift kommt für die Rechtssicherheit bei der Nutzung von De-Mail-Diensten eine hohe Bedeutung zu.

Zu § 7 (Verzeichnisdienst)

Der Verzeichnisdienst eröffnet dem Nutzer die Möglichkeit, seine Daten freiwillig so zu veröffentlichen, dass Dritte unabhängig von einer konkreten Kommunikationsbeziehung die Möglichkeit haben, sich über seine Identitätsdaten zu informieren. Zudem kann der Nutzer hier Informationen veröffentlichen, die Dritte benötigen, um dem Nutzer eine Ende-zu-Ende verschlüsselte Nachricht an sein Postfach zu senden („die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen“).

Gleichzeitig ist es dem Nutzer möglich, Daten, die nicht mehr zutreffen oder nicht mehr verwendet werden sollen, durch den akkreditierten Diensteanbieter löschen zu lassen; hierbei kann sich der Nutzer vertreten lassen, dabei gelten die Regelungen der §§ 164 folgende des Bürgerlichen Gesetzbuches.

Allein dadurch, dass ein Nutzer seine De-Mail-Adresse im Verzeichnisdienst nach § 7 veröffentlicht, hat er noch nicht den Zugang im Sinne von § 3a Absatz 1 des Verwaltungsverfahrensgesetzes eröffnet.

Zu Absatz 1

Satz 1 stellt klar, dass es dem Nutzer freigestellt ist, seine De-Mail-Adressen, die Identitätsdaten Name und Anschrift oder sonstige genannte Informationen im Verzeichnisdienst zu veröffentlichen. Ohne ein ausdrückliches Verlangen des Nutzers ist die Aufnahme im Verzeichnisdienst unzulässig; der Nutzer muss der Veröffentlichung explizit jeder einzelnen Information zustimmen, bevor sie im Verzeichnisdienst veröffentlicht wird. Satz 2 sieht vor, dass der akkreditierte Diensteanbieter sich das ausdrückliche Verlangen des Nutzers in eine Veröffentlichung seiner De-Mail-Adresse und seiner Identitätsdaten Name und Anschrift nicht auf dem Wege verschaffen darf, dass er hiervon die Eröffnung des De-Mail-Kontos, der in der Regel ein Vertragsabschluss zwischen Nutzer und akkreditiertem Diensteanbieter zugrunde liegen wird, für den Nutzer abhängig macht. Dieses Kopplungsverbot von De-Mail-Kontoeröffnung und ausdrücklichem Verlangen ist aufgrund seiner Einschränkung der Vertragsgestaltungsfreiheit auf die Fälle begrenzt, in denen dem Nutzer ein anderer Zugang zu gleichwertigen vertraglichen Gegenleistungen ohne das ausdrückliche Verlangen nicht oder nicht in zumutbarer Weise möglich ist. Die Formulierung lehnt sich damit an die bisherigen bereichsspezifischen Kopplungsverbote in § 95 Absatz 5

des Telekommunikationsgesetzes und in § 12 Absatz 3 des Telemediengesetzes an. Durch die Wörter „ohne das Verlangen“ soll die Konstellation erfasst werden, dass die marktbeteiligten akkreditierten Diensteanbieter für sich genommen jeweils keine marktbeherrschende Stellung besitzen und dem Nutzer daher ein Zugang zu gleichwertigen vertraglichen Leistungen an sich in zumutbarer Weise möglich ist, z. B. durch Absprachen unter den marktbeteiligten akkreditierten Diensteanbietern, aber marktweit immer nur, wenn er sein Verlangen äußert. Umgekehrt formuliert: Ein Zugang ist nicht in zumutbarer Weise möglich, wenn er nur mit ausdrücklichem Verlangen nach Absatz 1 Satz 1 möglich ist.

Zu Absatz 2

Die Regelung ist notwendig, um die informationelle Selbstbestimmung des Nutzers zu wahren und um zu verhindern, dass die De-Mail-Dienste unzutreffende Angaben verwenden. Dabei ist es unerheblich, ob die Daten absichtlich falsch angegeben oder irrtümlich falsche Angaben aufgenommen wurden. Weitergehende vertragliche Vereinbarungen, nach denen auch andere Personen eine Löschung veranlassen können, bleiben nach Satz 2 unbenommen. Die Löschung wird dadurch vollzogen, dass die De-Mail-Adresse, das Identitätsdatum oder die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen aus dem Verzeichnisdienst entfernt werden.

Zu § 8 (Dokumentenablage)

Das Angebot einer Dokumentenablage zur sicheren Ablage von elektronischen Dokumenten (Binär- oder Text-Dateien in beliebigem (Datei-) Format, neben Text-Dateien also z.B. auch Audio- oder Bild-Dateien) soll dem Nutzer ermöglichen, für ihn wichtige elektronische Dokumente zugriffsgesichert und gegen Verlust geschützt in seinem De-Mail-Konto aufzubewahren. Hierbei kann es sich um beliebige elektronische Dokumente handeln, zu denen der Zugriffsschutz über das Bestimmen einer sicheren Anmeldung individuell vom Nutzer festgelegt werden kann. Der Dienst trägt dem zunehmenden Bedürfnis der Nutzer Rechnung, wichtige elektronische Dokumente an einem sicheren Ort außerhalb des eigenen, stets gefährdeten Endgeräts gegen den etwaigen Verlust zu sichern, ohne dafür ein erhöhtes Risiko unbefugter Kenntnisnahme in Kauf nehmen zu müssen. Die sichere Dokumentenablage ist vom Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme geschützt. Es steht dem akkreditierten Diensteanbieter frei, diesen Dienst anzubieten. Bietet der akkreditierte Diensteanbieter eine Dokumentenablage an, so hat er zur Sicherung der elektronischen Dokumente dem Nutzer das Führen eines Protokolls über Änderungen und Neueinstellungen anzubieten, das durch eine dauerhaft überprüfbare qualifizierte Signatur gegen Manipulationen geschützt wird.

Zum Abschnitt 3 (De-Mail-Dienste-Nutzung)

Abschnitt 3 regelt Vorgaben an den akkreditierten Diensteanbieter, die sicherstellen sollen, dass die Vertrauenswürdigkeit seiner Dienste auch während der Nutzung seiner Dienste gewährleistet ist.

Zu § 9 (Aufklärungs- und Informationspflichten)

Der Nutzer ist das schwächste Glied in der Sicherheitskette der De-Mail-Dienste. Daher kommt seiner Unterrichtung über die erforderlichen Sicherheitsmaßnahmen durch den Diensteanbieter eine besondere Bedeutung zu. Die Unterrichtung hat in allgemein verständlicher Sprache zu erfolgen.

Zu Absatz 1

Absatz 1 normiert eine Unterrichtungspflicht des akkreditierten Diensteanbieters für den sicheren Zugang und die möglichen Rechtsfolgen eines unsicheren Zugangs. Der akkreditierte Diensteanbieter hat den Nutzer vor der erstmaligen Nutzung des De-Mail-Kontos über den sicheren Umgang mit den für die Nutzung des De-Mail-Dienstes notwendigen Zugangsinstrumenten zu unterrichten. Er muss ihn auf die Risiken hinweisen, die gegebenenfalls mit einer Weitergabe des Hardware-Token und des Passworts verbunden sind, und ihn darüber aufklären, wie er die Mittel zur Zugangssicherung aufbewahren und anwenden kann und welche Maßnahmen er im Verlustfalle oder bei Verdacht des Missbrauchs ergreifen muss. Andernfalls besteht die Gefahr, dass Unbefugte auf das De-MailKonto des Antragstellers zugreifen, in seinem Namen Nachrichten versenden oder sich mit seinen Identitätsdaten und seinen Attributen authentisieren.

Weiterhin hat der akkreditierte Diensteanbieter den Antragsteller auf mögliche Rechtsfolgen hinzuweisen, die mit der Nutzung des De-Mail-Dienstes verbunden sind. Zu diesen Rechtsfolgen gehört insbesondere die erhöhte Beweiswirkung der von Diensteanbietern erzeugten Zugangs- und Abholbestätigungen. Des Weiteren ist der Antragsteller darüber zu unterrichten, dass mit der Mitteilung der De-Mail-Adresse an eine staatliche Stelle dieser gegenüber ein Zugang nach § 3a Absatz 1 VwVfG e, § 87a Absatz 1 Satz 1 Abgabenordnung und § 36a Absatz 1 SGB I eröffnet und konkludent der Wille zum Empfang rechtlich verbindlicher Erklärungen bekundet wird.
Um eine rasche Akzeptanz beim Bürger zu erreichen, sollten im Sinne eines Gegenseitigkeitsprinzips Unternehmen darum bemüht sein, dass sie, wenn sie mit ihren Kunden per De-Mail kommunizieren, genauso den Empfang von De-Mail-Nachrichten ihrer Kunden akzeptieren. Zur Erreichung dieses Zieles sollte der akkreditierte Diensteanbieter – im eigenen Interesse zur raschen Verbreitung von De-Mail-Konten – seine Nutzer im Rahmen seiner Aufklärungspflichten darüber informieren, dass sie ihre Vertragspartner, die ihnen per De-Mail Nachrichten zusenden, dazu – etwa durch eine vertragliche Vereinbarung verpflichten, mit ihnen ebenfalls per De-Mail kommunizieren können und nicht auf die Web-Portale der Unternehmen verwiesen werden.

Zu Absatz 2

Dem Antragsteller ist nach Absatz 2 eine Belehrung in Textform gemäß § 126b des Bürgerlichen Gesetzbuchs zu übermitteln. Der Antragsteller hat deren Kenntnisnahme ausdrücklich zu bestätigen.

Zu § 10 (Sperrung und Auflösung des De-Mail-Kontos)

Für den Nutzer, den Diensteanbieter, betroffene Dritte und die zuständige Behörde müssen Möglichkeiten bestehen, die Rechtswirkungen von sicheren De-Mail-Diensten auch zu beenden.

Zu Absatz 1

Absatz 1 regelt die Voraussetzungen für eine Sperrung des Zugangs eines Nutzers zu einem De-Mail-Konto. Der akkreditierte Diensteanbieter ist zur Sperrung des Zugangs verpflichtet, wenn der Nutzer dies verlangt; hierbei kann der Nutzer sich vertreten lassen, dabei gelten die Regelungen der §§ 164 folgende des Bürgerlichen Gesetzbuches. Der Sperrantrag des Nutzers kann ohne Angabe von Gründen gestellt werden.

Die sichere Anmeldung zum De-Mail-Konto ist auch zu sperren, wenn die zur eindeutigen Identifizierung des Nutzers beim akkreditierten Diensteanbieter vorgehaltenen Daten nicht ausreichend fälschungssicher sind oder die sichere Anmeldung Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung des Anmeldevorgangs zulassen. In diesem Fall würde die Sperrung zu einem Zugangshindernis führen; hierüber ist der Sender einer Nachricht zu informieren. Da dem Diensteanbieter ermöglicht werden soll, auch weniger sichere Möglichkeiten der Anmeldung anzubieten, wird die Möglichkeit unbemerkter

Fälschung oder Kompromittierung einer solchen Anmeldung mit geringerer Sicherheit, die als solche gegenüber dem Rechtsverkehr kenntlich gemacht wird, nicht von der Regelung des Absatzes 1 Nr. 2 erfasst. Weiterhin kann die zuständige Behörde die Sperrung des Zugangs zum De-Mail-Konto anordnen.

Nach Absatz 1 Satz 2 kann der akkreditierte Diensteanbieter mit dem Nutzer weitere Sperrgründe vereinbaren. Denkbar ist beispielsweise eine Vereinbarung, die dem akkreditierten Diensteanbieter die Sperrung des Zugangs erlaubt, wenn der Nutzer mit der Zahlung eines Nutzungsentgelts in Verzug gerät.

Nach Absatz 1 Satz 3 ist der akkreditierte Diensteanbieter verpflichtet, eine Sperrung anzubieten, bei der der Nutzer trotz Sperrung in seinem Postfach eingegangene Nachrichten lesen kann. Diese Regelung ist notwendig, um z. B. zu verhindern, dass der Nutzer den Zugang einer in seinem Postfach abgelegten Nachricht nicht dadurch vereiteln kann, dass er die Sperrung des Zugangs zu seinem De-Mail-Konto verlangt oder die Sperrung durch den akkreditierten Diensteanbieter dadurch erwirkt, dass er mit der Zahlung des Nutzungsentgelts (absichtlich) in Verzug gerät. Der akkreditierte Diensteanbieter muss den Nutzer darüber informieren, dass er weiter Nachrichten empfangen und diese abrufen kann. Im Falle des Satzes 3, dass bei Sperrung lesender Zugang möglich bleibt, ist die Information des Senders darüber, dass die Nachricht nicht zugegangen sei, entbehrlich.

Absatz 1 Satz 4 dient dem Schutz des Nutzers. Die Bekanntgabe der Rufnummer (Telefonverbindung, „Sperr-Hotline“) soll eine unverzügliche Sperrung des Zugangs zum De-Mail-Konto ermöglichen. Eine Telefonverbindung erscheint hierzu am besten geeignet, weil eine solche im Gegensatz zu anderen Netzverbindungen nach gegenwärtigem Stand der Technik inzwischen praktisch überall und jederzeit schnell hergestellt werden kann. Der Sperrdienst des akkreditierten Diensteanbieters muss unter der Rufnummer jederzeit erreichbar sein. Eine vergleichbare Regelung findet sich in § 7 Absatz 1 der Signaturverordnung.

Zu Absatz 2

Absatz 2 stellt die Entscheidung, ob in den dort genannten Fällen eine Sperrung des De-Mail-Kontos geboten ist, in das pflichtgemäße Ermessen der zuständigen Behörde. Der Vorschrift kommt für die Rechtssicherheit bei der Nutzung von De-Mail-Diensten eine hohe Bedeutung zu.

Zu Absatz 3

Nach Absatz 3 hat der akkreditierte Diensteanbieter dem Nutzer erneut Zugang zum De-Mail-Konto zu gewähren, wenn der Grund für die Sperrung wegfällt. Hat beispielsweise der Nutzer die Sperrung des Zugangs verlangt, weil ihm der für den Zugang erforderliche Hardware-Token abhanden gekommen oder die Passwortinformation Dritten bekannt geworden ist, so ist ihm der Zugang bei Verwendung eines neuen Hardware-Token beziehungsweise nach Vergabe eines neuen Passworts zu ermöglichen.

Zu Absatz 4

Wird das De-Mail-Konto eines Nutzers nach Absatz 4 aufgelöst, so ist es endgültig gesperrt und nicht mehr nutzbar. Ein aufgelöstes Konto kann nicht wieder eröffnet werden. Die Auflösung erstreckt sich auf das gesamte De-Mail-Konto einschließlich des Zugangs zum Postfach- und Versanddienst sowie zu den Identitätsdaten.

Nach Satz 1 kann der Nutzer die Auflösung des De-Mail-Kontos verlangen; hierbei kann sich der Nutzer vertreten lassen, dabei gelten die Regelungen der §§ 164 folgende des Bürgerlichen Gesetzbuches. Eine Angabe von Gründen ist entbehrlich. Der Nutzer muss die Möglichkeit haben, die Benutzung seines De-Mail-Kontos endgültig einzustellen, indem er seine Auflösung beantragt und sich somit aus dem elektronischen Rechtsverkehr zurückzieht. Weiterhin kann die zuständige Behörde die Auflösung des De-Mail-Kontos anordnen. Die Hauptadresse im Sinne von § 5 Absatz 1 Satz 2 ist für 30 Jahre nach

Auflösung des entsprechenden De-Mail-Kontos gesperrt. Die Frist beginnt ab dem Zeitpunkt der Auflösung des De-Mail-Kontos zu laufen.

Ein Interesse des akkreditierten Diensteanbieters an einer Auflösung des De-Mail-Kontos eines Nutzers ist nicht ersichtlich. Weitere Auflösungsgründe können daher vertraglich nicht vereinbart werden.

Zu Absatz 5

Als Überprüfung der Identität („auf geeignete Weise“) kommen insbesondere Authentisierungsverfahren wie beispielsweise Passwortverfahren in Betracht. Dieses Verfahren ist zwischen dem Antragsteller und dem akkreditierten Diensteanbieter zu vereinbaren. Die Vereinbarung kann auch die Berechtigung weiterer Personen zur Sperrung einschließen. Eine vergleichbare Regelung findet sich in § 7 Absatz 2 der Signaturverordnung.

Zu Absatz 6

Absatz 6 regelt, unter welchen Voraussetzungen der akkreditierte Diensteanbieter den Eingang von Nachrichten an das Postfach eines gesperrten oder aufgelösten De-Mail-Kontos zu unterbinden und den Sender von der Unzustellbarkeit seiner Nachricht zu unterrichten hat. Dadurch, dass in diesen Fällen der Eingang von Nachrichten im Postfach verhindert wird, können sie dem Inhaber des De-Mail-Kontos auch nicht im Sinne von § 130 Absatz 1 Satz 1 BGB zugehen. Der Nutzer (hier als Empfänger) wird daher davor geschützt, dass er Erklärungen gegen sich gelten lassen muss, auf die er nicht zugreifen kann. Die Unterrichtung von der Unzustellbarkeit der Nachricht dient dem Schutz des Senders: Da seine Nachricht nicht zugeht, soll er durch den Hinweis auf die Unzustellbarkeit die Gelegenheit erhalten, seine Nachricht dem Nutzer (als Empfänger) über einen anderen Kommunikationskanal zu übermitteln.

Zu § 11 (Einstellung der Tätigkeit)

Die Regelungen sollen der Wahrung der Interessen der Nutzer von De-Mail-Diensten dienen. Es soll sichergestellt werden, dass der Zugang zu einem De-Mail-Konto auch nach Beendigung der Tätigkeit eines akkreditierten Diensteanbieters möglich ist. Es kann nicht ausgeschlossen werden, dass akkreditierte Diensteanbieter bereits nach kurzer Zeit wieder aus dem Markt ausscheiden. Eine generelle Übernahmeverpflichtung für die zuständige Behörde würde jedoch eine nicht übersehbare Belastung bedeuten. Die Vorschrift des Absatzes 2 dient daher dem Schutz des Nutzers vor dem Risiko eines Datenverlusts für den Fall, dass kein anderer akkreditierter Diensteanbieter das De-Mail-Konto übernimmt. Absatz 1 Satz 1 und 3 sowie Absatz 2 sind bußgeldbewehrt (s. § 23 Absatz 1 Nummern 5 bis 7).

Zu § 12 (Vertragsbeendigung)

Die Regelung ist notwendig, um das gegenüber herkömmlichen Diensten erhöhte Vertrauen in den De-Mail-Dienst eines akkreditierten Diensteanbieters zu rechtfertigen und die elektronische Mobilität des Nutzers – etwa im Fall eines Anbieterwechsels – zu gewährleisten. Um sicherzustellen, dass der akkreditierte Diensteanbieter seiner gesetzlichen Verpflichtung tatsächlich nachkommt, ist die Regelung bußgeldbewehrt (s. § 23 Absatz 1 Nummer. 8).

Zu § 13 (Dokumentation)

Die Dokumentation soll vor allem dazu beitragen, dass wirksame Kontrollen durchgeführt und mögliche gegebenenfalls auch haftungsrelevante Pflichtverletzungen festgestellt werden können. Dokumentiert werden soll z.B. die im Rahmen der Eröffnung eines De-Mail-Kontos nach § 3 erfolgte Identifizierung, die Erhebung, die Änderung und Sperrung von

entsprechenden Attributen sowie jede Änderung an einem Vertragsverhältnis. Die Dokumentation kann im Streitfall vor Gericht als wichtiges Beweismittel dienen. Mit der Bußgeldvorschrift nach § 23 kommt der Dokumentation zusätzliche Bedeutung zu. Die Absätze 1 und 2 sind bußgeldbewehrt (s. § 23 Absatz 1 Nrn. 9 und 10).

Zu Absatz 1

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 (Beispiel: Sperrung? Kündigung des der De-Mail-Nutzung zugrundeliegenden Vertrages?). Hierbei beinhaltet die Dokumentationspflicht

- hinsichtlich der Eröffnung eines De-Mail-Kontos durch natürliche Personen eine Ablichtung des vorgelegten Ausweises oder anderer Identitätsnachweise, es sei denn die Überprüfung der Identität erfolgt mittels des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes; das Protokoll der Identifizierung einschließlich der Prüfprotokolle bei der Nutzung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes; die beantragte Hauptadresse im Sinne des § 5 Absatz 1; ggf. die beantragte Pseudonym-Adresse(n); das Datum der Beantragung auf Eröffnung eines De-Mail-Kontos; den Nachweis über die Unterrichtung des Antragstellers nach § 9 des De-Mail-Gesetzes; die Identifizierungsdaten zum bearbeitenden Mitarbeiter des akkreditierten Diensteanbieters (wenn eine manuelle Bearbeitung erfolgt); die erfassten Antragsdaten hinsichtlich aller Identitätsattribute (z.B. Vorname, Nachname, Geburtsort, Geburtsdatum, Ausweisdaten, Wohnort).

- Hinsichtlich der Eröffnung eines De-Mail-Kontos durch juristische Personen, Personengesellschaften oder öffentliche Stellen einen Nachweis über die Identität des Unternehmens oder der öffentlichen Stelle, der nicht älter als ein Monat sein darf; eine beglaubigte Abschrift des Vertretungsnachweises, sofern dies nicht durch einen Registereintrag nachvollzogen werden kann; eine Ablichtung des vorgelegten Ausweises oder anderer Identitätsnachweise der vertretungsberechtigten natürlichen Person, es sei denn die Überprüfung der Identität erfolgt mittels des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes; das Protokoll der Identifizierung, einschließlich der Prüfprotokolle bei der Nutzung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes; die beantragte De-Mail-Domain, die Bestandteil der De-Mail-Adresse werden soll; das Datum der Beantragung auf Eröffnung eines De-Mail-Kontos; den Nachweis über die Unterrichtung des Antragstellers nach § 9 des De-Mail-Gesetzes; die Identifizierungsdaten zum bearbeitenden Mitarbeiter des akkreditierten Diensteanbieters (wenn eine manuelle Bearbeitung erfolgt); die erfassten Antragsdaten hinsichtlich aller Identitätsattribute (z.B. Name, Anschrift, Angaben zur vertretungsberechtigten Person (Vorname, Nachname, Geburtsort, Geburtsdatum, Ausweisdaten, ...), Rechtsform).

- hinsichtlich der Änderung von Daten, die hinsichtlich der Führung eines De-Mail-Kontos relevant sind, sowie hinsichtlich der Änderung des Status‘ eines De-Mail-Kontos das betroffene De-Mail-Konto inkl. der De-Mail-Adresse; den akkreditierten Diensteanbieter; die jeweilige gesetzliche Zeit der Änderung, die Identifizierungsdaten zur die Änderung beantragenden natürlichen oder juristischen Person, Personengesellschaft oder öffentlichen Stelle bzw. ob die Änderung auf Veranlassung oder . Anordnung der zuständigen Behörde erfolgt ist (z.B. Sperrung oder Auflösung eines De-Mail-Kontos nach § 10); die Art der Verarbeitung (automatisiert, manuell); die Identifizierungsdaten zum bearbeitenden Mitarbeiter des akkreditierten Diensteanbieters (wenn eine manuelle Bearbeitung erfolgt); die Art der Verwaltung/Änderungen (z.B. Änderung, Auflösung, Hinzufügen, Identifizierung, Verifizierung, Freischaltung, Sperrung inkl. Sperrart, Entsperrung); die erfassten Änderungsdaten hinsichtlich aller Identitätsattribute, zugeordneter De-Mail-Adressen (z.B. Vorname, Nachname, Geburtsort, Geburtsdatum, Ausweisdaten, Wohnort, DM-Domain, primäre De-Mail-Adresse, Pseudonym-De-Mail-

Adresse, Rechtsform der juristischen Person, Personengesellschaft oder öffentlichen Stelle).

Die Dokumentation muss so erfolgen, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Soweit die Dokumentation elektronisch erfolgt, soll sie mit qualifizierten Zeitstempeln versehen werden, so dass ihr die Beweiswirkungen des § 371a der Zivilprozessordnung zukommen.

Zu Absatz 2

Absatz 2 normiert die für die Dokumentation des akkreditierten Diensteanbieters geltende Aufbewahrungsfrist. Diese endet nach Ablauf von 30 Jahren nach dem Schluss des Jahres, in dem das zwischen dem Nutzer und dem akkreditierten Diensteanbieter begründete Vertragsverhältnis endet. Da Schadensersatzansprüche unter den Voraussetzungen von § 199 Absatz 3 Satz 1 Nummer 2 des Bürgerlichen Gesetzbuches erst 30 Jahre nach dem den Schaden auslösenden Ereignis verjähren, ist diese Aufbewahrungsfrist sachgerecht.

Zu Absatz 3

Absatz 3 verpflichtet den Diensteanbieter, dem Nutzer Einsicht in die ihn betreffenden Daten zu gewähren. Die Vorschrift eröffnet dem Nutzer die Möglichkeit, sich von der Korrektheit der ihn betreffenden Daten und Verfahrensschritte (z.B. der unverzüglichen Durchführung einer beantragten Zugangssperrung nach § 10 Absatz 1) zu überzeugen, ohne ein Gerichtsverfahren anstrengen zu müssen. Dies dient dem Vertrauensschutz und der Entlastung der Gerichte.

Zu § 14 (Jugend- und Verbraucherschutz)

Die Vorschrift betont den Gedanken des Verbraucherschutzes. Gerade mit Blick auf die Vertrauenswürdigkeit der De-Mail-Dienste ist die Einhaltung der verbraucherschutzrechtlichen Vorschriften von großer Bedeutung. Die in der Norm vorgenommene Aufzählung verbraucherschützender Vorschriften ist exemplarisch und weder im Verhältnis zwischen akkreditiertem Diensteanbieter und Nutzer noch im Verhältnis zwischen akkreditiertem Diensteanbieter und Dritten abschließend.

Zu § 15 (Datenschutz)

Die Regelung soll die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Bereitstellung der akkreditierten De-Mail-Dienste und deren Durchführung auf das Notwendige begrenzen. Die Erhebung soll grundsätzlich beim betroffenen Nutzer eines De-Mail-Kontos erfolgen. Vorrangig gelten die allgemeinen Datenschutzvorschriften insbesondere des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes; die Regelung hat insofern Auffangcharakter. Die Regelung findet Anwendung auf solche (Teil-)Dienste der De-Mail-Dienste, welche nicht schon Gegenstand des Telemediengesetzes, des Telekommunikationsgesetzes oder des Bundesdatenschutzgesetzes sind.

Zu § 16 (Auskunftsanspruch)

Nach § 5 Absatz 2 sind können akkreditierte Diensteanbieter anbieten, die Wahrnehmung der De-Mail-Dienste auch pseudonym zu ermöglichen. Dritte können diese Pseudonyme im Rechtsverkehr als datenschutzfördernde Alternative nur akzeptieren, wenn sie sicher sein können, dass ihnen zur Durchsetzung ihrer Anspräche gegebenenfalls ein Aufdeckungsanspruch zusteht. Die Regelung sieht einen Auskunftsanspruch vor, mit welchem der auskunftsuchende Dritte Namen und Anschrift und damit die Aufdeckung der ladungsfähigen Anschrift des pseudonymen Nutzers erhält. Die Auskunft über die ladungsfähige Anschrift kann in Streitfällen erforderlich sein, etwa wenn der pseudonyme

Nutzer seinen Pflichten aus einem über eine De-Mail-Korrespondenz zustande gekommenen Vertrag nicht nachkommt.

Der Auskunftsanspruch ist mit wirksamen Restriktionen zu versehen, um den Schutz der Pseudonymität zu gewährleisten. Zu niedrige Voraussetzungen würden das Pseudonym von Anfang an personenbeziehbar machen, so dass es sich von Anfang an nicht um Pseudonyme handeln würde. Die hier getroffene Regelung trägt darüber hinaus den Interessen der akkreditierten Diensteanbieter Rechnung, die das Vorliegen der Voraussetzungen eines Auskunftsanspruchs zu prüfen haben und nicht mit einer zu weit gehenden Prüfungspflicht belastet werden können. Die Auskunftsvoraussetzungen können dienstübergreifend geregelt werden, da sich insoweit keine Notwendigkeit einer Differenzierung nach Diensten ergibt.

Zu Absatz 1

Für den privaten Auskunftsanspruch ist das Vorliegen eines Rechts, zu dessen Durchsetzung die Auskunft erforderlich ist, glaubhaft darzulegen. In den meisten Fällen wird es möglich sein, diesen Anspruch mittels der unter dem Pseudonym geführten Kommunikation darzulegen. Dem Anspruchsteller wird die Auskunftserlangung daher nicht so sehr erschwert, dass er bei der Verwendung von Pseudonymen um die Durchsetzungsfähigkeit seiner Ansprüche fürchten müsste. Auf der anderen Seite muss so jedoch eine tatsächliche Beziehung zum Nutzer nachgewiesen werden. Für den akkreditierten Diensteanbieter ergibt sich eine ausreichend begrenzte Prüftiefe.

Der Nachweis einer Rechtsverfolgung ist jedoch erforderlich, da ansonsten schon bei jeder tatsächlichen Personenbeziehung ein Auskunftsanspruch ermöglicht würde. Um einem Missbrauch des Auskunftsanspruches vorzubeugen, ist die Auskunftserteilung davon abhängig zu machen, dass sich der akkreditierte Diensteanbieter über die Identität des Auskunftssuchenden in entsprechender Anwendung von § 3 Absatz 2 und 3 vergewissert.

Zu Absatz 2

Absatz 2 regelt eine Haftungserleichterung für den Fall, dass der akkreditierte Diensteanbieter einem unberechtigten Auskunftsverlangen nachkommt und sich deshalb Regressforderungen des Nutzers, über dessen Namen und Anschrift Auskunft erteilt wurde, gegenübersieht. Die Beschränkung der Haftung auf Vorsatz, die nur für wahrheitsgemäße Angaben gilt, trägt dem Umstand Rechnung, dass es für den akkreditierten Diensteanbieter schwierig sein kann zu beurteilen, ob die Voraussetzungen des Absatzes 1 vorliegen. Die Vorschrift ist keine eigene Anspruchsgrundlage für Forderungen des pseudonymen Nutzers, über dessen Namen und Anschrift Auskunft gegeben wird.

Zu Absatz 3

Absatz 3 sichert durch eine strenge Zweckbindung die Begrenzung des Auskunftsanspruchs auf einen konkrete Zweck und einen bestimmbaren Personenkreis. Dem Ersuchenden soll nicht ermöglicht werden, das Pseudonym auch für weitere Personen aufzudecken.

Zu Absatz 4

Die Auskunftspraxis des akkreditierten Diensteanbieters muss jedoch für den Nutzer transparent und überprüfbar bleiben. Daher wird der akkreditierte Diensteanbieter in Absatz 4 verpflichtet, den Nutzer über die Auskunftserteilung zu informieren. Die Dokumentation ermöglicht es dem Nutzer, die Berechtigung der Auskunftserteilung im Nachhinein zu prüfen. Eine Benachrichtigung des Nutzers vor der Auskunftserteilung und das Durchführen eines kontradiktorischen Verfahrens würde jedoch den akkreditierten Diensteanbieter zu weitgehend belasten und diesem Aufgaben auferlegen, zu deren Bewältigung er nicht sachgemäß gerüstet wäre. Die aufgezählten Inhalte der Dokumentation sind erforderlich, um dem Nutzer die Prüfung der Berechtigung der Auskunftserteilung zu ermöglichen. Die Begrenzung der Aufbewahrungspflicht auf zwölf Monate entspricht der Aufbewahrungsdauer vergleichbarer Dokumentationsinhalte (vgl. § 8 Absatz 3 Satz 3 der Signaturverordnung) und

ist in seiner Kürze gerechtfertigt, da der Nutzer unverzüglich über eine Auskunftserteilung in Kenntnis gesetzt werden muss.

Zu Absatz 5

Absatz 5 dient der Aufwandsentschädigung des akkreditierten Diensteanbieters. Außerdem stellt die Kostenpflichtigkeit der Auskunft eine weitere Hürde für massenweises Auskunftsersuchen dar. Die Kostenerstattung ist jedoch auf den tatsächlichen Aufwand beschränkt. Die Rechtsdurchsetzung soll andererseits nicht durch überhöhte Kosten erschwert werden.

Zu Absatz 6

In Absatz 6 wird klargestellt, dass die nach anderen Rechtsvorschriften bestehenden Regelungen zu Auskünften gegenüber öffentlichen Stellen (z. B. nach § 14 Absatz 2 Telemediengesetz, gegebenenfalls in Verbindung mit weiteren Fachgesetzen) unberührt bleiben.

Zum Abschnitt 4 (Akkreditierung)

Der Aufbau einer Infrastruktur von De-Mail-Diensten ist auf die private Initiative der Diensteanbieter und das Vertrauen der Nutzer angewiesen. Um beides zu erleichtern, ist es erforderlich, einen verlässlichen Nachweis der überprüften Vertrauenswürdigkeit der angebotenen Dienste als Infrastrukturleistung des Staates anzubieten. Wer die Verfügbarkeit, die Sicherheit und den Datenschutz seiner Dienste sowie ihr Zusammenwirken mit anderen De-Mail-Diensten überprüfen und bestätigen lassen möchte, kann die Akkreditierung und damit das staatliche Gütezeichen für vertrauenswürdige De-Mail-Dienste beantragen und mit diesem auf dem Markt um das Vertrauen seiner Kunden werben. Staatliche und private Stellen können die nachgewiesene Vertrauenswürdigkeit der akkreditierten Diensteanbieter in ihren Informatikanwendungen berücksichtigen.

Zu § 17 (Akkreditierung von Diensteanbietern)

Die Vorschrift dient der Einführung eines Akkreditierungssystems. Dieses dient der Qualitätssicherung und dem Nachweis dieser Qualität im Rechts- und Geschäftsverkehr. Die Akkreditierung soll durch die vorangegangene Prüfung des akkreditierten Dienstanbieters die Vertrauenswürdigkeit gewährleisten, die benötigt wird, um bestimmte Rechtsfolgen an die Verwendung von De-Mail-Diensten zu knüpfen. Die Bedeutung der Akkreditierung beruht darauf, dass die Erfüllung der gesetzlichen Anforderungen vorab und auch danach in regelmäßigen Zeitabständen sowie bei wesentlichen Veränderungen des Dienstes durch öffentlich anerkannte fachkundige Dritte umfassend geprüft und bestätigt wird. Bei der Akkreditierung handelt es sich um einen Verwaltungsakt.

Zu Absatz 1

Absatz 1 regelt das Antragserfordernis für das Akkreditierungsverfahren. Satz 2 gewährleistet dem Antragsteller einen Rechtsanspruch auf Akkreditierung, wenn er die Erfüllung der genannten Anforderungen nachweisen kann. Gelingt ihm dies nicht, ist die Akkreditierung zu versagen. Zudem muss sichergestellt sein, dass die zuständige Behörde die Aufsicht über den akkreditierten Diensteanbieter effektiv ausüben kann. Dafür ist es erforderlich, dass der Diensteanbieter eine Niederlassung oder einen Wohnsitz im Inland hat. Dies ist insbesondere vor dem Hintergrund erforderlich, dass der akkreditierte Diensteanbieter nach § 5 Absatz 6 Satz 2 als beliehener Unternehmer tätig wird und damit eine effektive Ausübung der Aufsicht notwendig ist. Sätze 3 bis 6 betreffen den Nachweis der geprüften und bestätigten Vertrauenswürdigkeit im Rechts- und Geschäftsverkehr. Das Gütezeichen und die weiteren Kennzeichnungen, die einen akkreditierten Diensteanbieter als solchen kenntlich machen, soll die Verwendung von sicheren De-Mail-Diensten fördern.

Eine weitere Kennzeichnung ist z.B. in § 5 Absatz 1 Satz 2 genannt. Die Kennzeichnung führt zu Markttransparenz und Rechtssicherheit, die für einen ausreichenden Vertrauensschutz im täglichen Rechts- und Geschäftsverkehr erforderlich sind und die dem Schutzbedarf im elektronischen Rechts- und Geschäftsverkehr Rechnung tragen. Es ist zu erwarten, dass die Gerichte der Prüfung und der Bestätigung der Vertrauenswürdigkeit durch die zuständige Behörde Vertrauen entgegen bringen und ihm einen besonders hohen Beweiswert zumessen werden. Der durch die Prüfung und Bestätigung entstehende Anschein der Vertrauenswürdigkeit kann allerdings nur soweit reichen, wie die Anforderungen des Gesetzes für die einzelnen De-Mail-Dienste Anknüpfungspunkte für einen solchen Anschein bereithalten. Die Regelung des Satzes 6 ist bußgeldbewehrt (vgl. § 23 Absatz 1 Nummer 11).

Zu Absatz 2

Um die fortdauernde Vertrauenswürdigkeit im weiteren Betrieb zu gewährleisten, sind nach wesentlichen Veränderungen der für die Akkreditierung bestätigten Umstände, spätestens aber nach drei Jahren die Überprüfungen zu erneuern und aktuelle Bestätigungen über das Vorliegen der Akkreditierungsvoraussetzungen vorzulegen. Wesentliche Veränderungen sind insbesondere bei sicherheits- oder schutzerheblichen Änderungen in Technik, Organisation und Geschäftsmodellen der De-Mail-Dienste anzunehmen (z.B. Änderungen eines eingesetzten Produktes, Umzug des Rechenzentrums, Beauftragung eines Dritten), können sich aber auch auf alle anderen Voraussetzungen, die sich aus § 18 ergeben, beziehen. Anknüpfungspunkt für die wesentlichen Veränderungen kann also auch der Diensteanbieter selbst sein.

Zu Absatz 3

Behörden des Bundes, der Länder und Kommunen bieten kraft ihrer Stellung die Gewähr, dass die Voraussetzungen nach § 18 Absatz 1 Nr. 1 und Nr. 2 erfüllt sind, sie müssen daher im Rahmen des Akkreditierungsverfahrens nicht nachgewiesen werden.

Zu § 18 (Voraussetzungen der Akkreditierung; Nachweis)

Die Vorschrift regelt die Voraussetzungen für eine Akkreditierung und trifft nähere Bestimmungen dazu, in welcher Weise die Erfüllung dieser Voraussetzungen nachgewiesen werden kann.

Zu Absatz 1

Absatz 1 regelt die Voraussetzungen der Akkreditierung.

Zu Nummer 1

Nummer 1 regelt die Voraussetzungen der Akkreditierung, die in der Person des Diensteanbieters und der in seinem Betrieb tätigen Personen, die für das Angebot und den Betrieb des De-Mail-Dienstes zuständig sind, erfüllt sein müssen. Dies umfasst die allgemeine Zuverlässigkeit und die Fachkunde in dem jeweiligen Tätigkeitsbereich. Zuverlässigkeit und Fachkunde sind auf den Betrieb von De-Mail-Diensten bezogen. Die erforderliche Zuverlässigkeit besitzt insbesondere, wer auf Grund seiner persönlichen Eigenschaften oder der persönlichen Eigenschaften der in seinem Betrieb tätigen Personen, seines Verhaltens und seiner Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist.
Die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit besitzen in der Regel Personen nicht, die

1. wegen Verletzung der Vorschriften

   a. des Strafrechts über den Schutz des persönlichen Lebens- und Geheimbereichs, Eigentums- und Vermögensdelikte, Urkundendelikte und Insolvenzstraftaten
   b. des Datenschutzrechts,
   c. des Gewerberechts

   mit einer Strafe oder in den Fällen der Buchstaben b und c zu einer Geldbuße in Höhe von mehr als tausend Deutsche Mark oder fünfhundert Euro belegt worden ist,
2. wiederholt oder grob pflichtwidrig
   a. gegen Vorschriften nach Nummer 1 Buchstabe b und c verstoßen hat oder
   b. seine Verpflichtungen als Beauftragter für den Datenschutz verletzt hat,
3. infolge strafgerichtlicher Verurteilung die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,
4. sich nicht in geordneten wirtschaftlichen Verhältnissen befindet, es sei denn, dass dadurch die Interessen der Nutzer oder anderer Personen nicht gefährdet sind, oder
5. aus gesundheitlichen Gründen nicht nur vorübergehend unfähig ist, die Aufgaben eines akkreditierten Diensteanbieters ordnungsgemäß auszuüben.

Als weiter Maßstab wird auf. § 5 Absatz 2 Nummer 1 a), d) und e) sowie Nummern 3 bis 5 Umweltauditgesetz in der Fassung der Bekanntmachung vom 4. September 2002 (BGBl. I S.3490), zuletzt geändert durch Artikel 11 des Gesetzes vom 17. März 2008 (BGBl. I S. 399), oder des Vorbildes von §§ 5 und 6 Waffengesetz vom 11. Oktober 2002 (BGBl. I S. 3970 (4592) (2003, 1957)), zuletzt geändert durch Artikel 1 des Gesetzes vom 26. März 2008 (BGBl. I S. 426), hingewiesen.

Zu Nummer 2

Der Diensteanbieter muss sicherstellen, dass er über hinreichend finanzielle Mittel verfügt, um gegen ihn gerichtete Schadensersatzforderungen erfüllen zu können. Zu diesem Zweck wird er im Rahmen der Akkreditierung verpflichtet, eine geeignete Deckungsvorsorge zu treffen.

Zu Nummer 3

Der Diensteanbieter kann grundsätzlich nur akkreditiert werden, wenn er die in §§ 3 bis 13 sowie § 16 genannten Pflichten erfüllt und die dort genannten Pflichtdienstleistungen anbietet. Ein Diensteanbieter kann nach Halbsatz 2 auch akkreditiert werden, wenn er allein den Dienst Postfach- und Versanddienst (§ 5) anbietet; ob er zusätzlich den Identitätsbestätigungsdienst (§ 6) oder den Dienst Dokumentenablage (§ 8) anbietet, bleibt ihm überlassen. Die für ein akkreditiertes De-Mail-Dienste-Angebot konstitutiven Dienste müssen sicher, zuverlässig und im Zusammenwirken mit den anderen akkreditierten Diensteanbietern erbracht werden. Dabei bezieht sich die Gewährleistung des Zusammenwirkens sowohl auf die technische und organisatorische Ebene als auch auf die Gestaltung der Vergütungsmodelle und den Ausgleich entstehender Kosten. Ziel ist eine von allen akkreditierten Diensteanbietern getragene Infrastruktur vertrauenswürdiger De-Mail-Dienste.

Die Beschränkung der zulässigen Standorte für die von den akkreditierten Diensteanbietern verwendeten Server auf das Territorium der Mitgliedstaaten der EU dient dem Datenschutz und der Datensicherheit hinsichtlich der über De-Mail-Dienste versandten Nachrichten sowie der in den Dokumentenablagen der akkreditierten Diensteanbieter abgelegten elektronischen Dokumente. Eine effektive Kontrolle der Sicherheit von außerhalb der EU befindlichen Servern würde für Behörden der Mitgliedsstaaten unmöglich. In Ermangelung einer solchen Kontrolle besteht Grund zu der Befürchtung, dass die Server einem erhöhten Angriffsrisiko ausgesetzt wären. Dieses Angriffsrisiko muss aber so gering wie möglich gehalten werden, damit eine rechtssichere und rechtsverbindliche Kommunikation über De-Mail-Dienste gewährleistet ist und die in den Dokumentenablagen abgelegten Daten langfristig manipulationsfrei verfügbar sind. Zu den vom akkreditierten Diensteanbieter verwendeten Servern gehören insbesondere die Geräte, auf denen die Identitätsdaten gespeichert sowie

die Postfächer und die Dokumentenablage nach § 8 vorgehalten werden. Die Vorschrift erfasst hingegen nicht solche Server, die beim Transport der über De-Mail-Dienste versandten Nachrichten lediglich für die Weiterleitung im Internet verwendet werden, denn nach dem derzeitigen Stand der Technik ist der Transportweg der Nachrichten nicht vorhersehbar. Da der akkreditierte Anbieter die Nachrichten mit einer Transportverschlüsselung versieht, wird die Datensicherheit durch die Verwendung von außerhalb der EU befindlichen Weiterleitungs-Servern auch nicht beeinträchtigt. Ebenfalls nicht von der Regelung erfasst sind Rechner, die der Nutzer verwendet, um auf sein De-Mail-Konto zuzugreifen.

Zu Nummer 4

Zu den Voraussetzungen für die Akkreditierung gehört auch die Erfüllung der datenschutzrechtlichen Anforderungen für die Gestaltung und den Betrieb der Dienste (vgl. auch § 15). Dies umfasst insbesondere die Beachtung der informationellen Selbstbestimmung der Betroffenen nach Maßgabe der datenschutzrechtlichen Bestimmungen und die Gewährleistung ausreichender Sicherheit für die über die De-Mail-Dienste verarbeiteten personenbezogenen Daten. Hierzu gehört auch die datenschutzgerechte Gestaltung der Dienste insbesondere durch das Angebot pseudonymer Nutzungsmöglichkeiten der einzelnen Dienste und den Schutz der Pseudonymität.

Zu Absatz 2

Das den De-Mail-Diensten zugrunde liegende technische Konzept ist komplex und ist in der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik zur Umsetzung durch die einzelnen Beteiligten detailliert niedergelegt. Datenschutz und Datensicherheit des technischen Systems „De-Mail“ hängen wesentlich von ihrer Umsetzung nach dem Stand der Technik ab. Die Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik enthält daher ausführliche Hinweise auf eine Umsetzung nach dem Stand der Technik. § 18 Absatz 2 enthält die zentrale Verweisungsnorm auf diese Richtlinie. Um das System flexibel zu halten und im Rahmen des technischen Fortschritts Weiterentwicklungen zu ermöglichen, wird dynamisch auf die jeweils aktuelle im elektronischen Bundesanzeiger veröffentlichte Fassung der Richtlinie verwiesen.

Bevor das BSI wesentliche Änderungen an der Technischen Richtlinie vornimmt, hört es den Ausschuss De-Mail-Standardisierung nach § 22 an. Bei der Frage der Bewertung der Wesentlichkeit ist die Bedeutung der Kostenintensität der jeweiligen Umsetzung zu berücksichtigen und ins Verhältnis der dafür gewonnenen Verbesserung in Sicherheit, Funktionalität oder Datenschutz zu setzen. Mit der Beteiligung soll gewährleistet sein, dass rechtzeitig Fachwissen insbesondere der betroffenen Wirtschaft an das BSI gelangt.

Die Norm orientiert sich im Wesentlichen an § 2 der Personalausweisverordnung.

Zu Absatz 3

Die Vorschrift trifft nähere Bestimmungen dazu, wie neben den allgemeinen Nachweisen der Identität des Antragstellers (zum Beispiel durch Auszüge aus dem Handelsregister) die in Absatz 1 geregelten allgemeinen Anforderungen an Diensteanbieter und ihre Dienste nachgewiesen werden können. Dies ist erforderlich, um die Prüftiefe für die Akkreditierung zu bestimmen. Um das in sie gesetzte Vertrauen, auch mit Blick auf anknüpfende, unter Umständen auch belastende Rechtsfolgen, zu rechtfertigen, bedarf es einer objektiv nachweisbaren und nachvollziehbaren Prüfung vor der Akkreditierung.

Zu Nummer 1

Die für den Betrieb erforderliche Zuverlässigkeit wird angenommen, wenn keine Hinweise, die hieran Zweifel begründen, vorliegen. Zum Nachweis dient in der Regel ein Führungszeugnis nach § 30 Absatz 5 Bundeszentralregistergesetz. Weitere Nachweise (etwa zur allgemeinen finanziellen Situation) können verlangt werden, wenn hierzu ein konkreter Anlass besteht. Der Nachweis der erforderlichen technischen, administrativen und/oder juristischen Fachkunde erfolgt durch Vorlage von Zeugnissen über Aus- und Fortbildungen, die der jeweiligen konkreten Tätigkeitsbeschreibung entsprechen. Die Nachweise sind für sämtliche Mitarbeiter, die mit sicherheitskritischen Tätigkeiten betraut sind, zu erbringen. Die akkreditierten Diensteanbieter sollen zudem durch regelmäßige Schulungen zur Gewährleistung der fachlichen Eignung der von ihnen eingesetzten Mitarbeiter beitragen.

Zu Nummer 2

Die Erfüllung der Verpflichtung, eine geeignete Deckungsvorsorge zu treffen, wird durch die Vorlage der Urkunde eines entsprechenden Vertrags mit einer Versicherungsgesellschaft oder einem Kreditinstitut nachgewiesen. Die Überprüfung stellt sicher, dass die akkreditierten Diensteanbieter im Falle einer gesetzlichen Haftung ihre Verpflichtung erfüllen können. Mit Blick auf Artikel 14 Absatz 7 der Dienstleistungsrichtlinie ist eine Beschränkung auf zugelassene inländische Unternehmen nicht zulässig. Der Vertrag über eine Deckungsvorsorge kann daher mit jedem Anbieter innerhalb der europäischen Gemeinschaften geschlossen werden.

Die Mindestdeckungssumme gilt für den einzelnen Schadensfall. Ein auslösendes Ereignis (zum Beispiel eine fehlerhafte Identifizierung, ein Fehler im Postfach- und Versanddienstsystem oder eine nicht vollzogene Sperrung) kann zu einer Vielzahl von Einzelschäden führen. Da Anzahl und Höhe potentieller Schäden nur schwer vorhersehbar sind, kommt zur Deckungsvorsorge vor allem eine entsprechende Versicherung in Betracht. Alternativ kann die Deckungsvorsorge auch in einer entsprechend hohen Kapitaldeckung durch ein Kreditinstitut bestehen.

Die vorgesehene Mindestdeckungssumme ist angemessen. Sie deckt auf der einen Seite die üblichen Rahmen von geldwerten Transaktionen, wie zum Beispiel beim Online-Banking, ab und hält auf der anderen Seite die erforderliche Deckungsvorsorge für die akkreditierten Diensteanbieter in vertretbaren Grenzen.

Zu Nummer 3

Die Erfüllung der Anforderungen an einen vollständigen, zuverlässigen, kooperativen, kompatiblen und sicheren Betrieb des De-Mail-Dienste-Angebots können durch Sicherheitszertifikate nach § 9 des Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik nachgewiesen werden. Die Zertifizierung erfolgt aufgrund einer Technischen Richtlinie De-Mail/Bürgerportal, die vom BSI als die für die Sicherheitszertifikate zuständige Stelle festgelegt wird.

Nachgewiesen werden muss zum einen, dass der Diensteanbieter die in den §§ 3 bis 5 und § 7 genannten Pflichtdienste der sicheren Identifizierung (bei Eröffnung des De-Mail-Kontos, § 3), der sicheren Anmeldung (§ 4), des sicheren Postfachs und Versands (§ 5), des sicheren Verzeichnis- und Sperrdienstes (§ 7) und – gegebenenfalls – des sicheren Identitätsbestätigungsdienstes (§ 6) und des sicheren Dienstes Dokumentenablage (§ 8) unter Erfüllung der genannten Anforderungen anbietet und die weiteren in §§ 9 bis 13 und § 16 genannten Pflichten erfüllt.

Zum anderen ist auf der Basis ausreichender Tests zu bestätigen, dass der Diensteanbieter die jederzeitige Verfügbarkeit dieser Dienste gewährleistet und dass diese mit den entsprechenden Diensten der anderen akkreditierten Diensteanbieter auf der Basis gemeinsamer Standards zusammenarbeiten.

Schließlich ist zu bestätigen, dass diese Dienste technisch und organisatorisch sicher erbracht werden. Kern der Sicherheitsgewährleistung ist ein umfassendes Sicherheitskonzept, dessen Eignung und Umsetzung nachzuweisen ist. Aktuelle Sicherheitszertifikate zu Teilfunktionen des Sicherheitskonzepts, wie etwa ein Grundschutzzertifikat, oder zu eingesetzten Technikprodukten können in den Nachweis einbezogen werden, um Doppelprüfungen zu vermeiden. Die Prüfung des Sicherheitskonzeptes kann sich dann auf die nicht von den Zertifikaten erfassten Funktionen und Produkte und das dienstbezogene Zusammenwirken aller Komponenten beschränken.

Zu Nummer 4

Zu den Voraussetzungen für die Akkreditierung gehört neben den Anforderungen an die Datensicherheit (§ 9 BDSG), die in Nummer 3 geregelt sind, auch die Erfüllung der datenschutzrechtlichen Anforderungen für die Gestaltung und den Betrieb der Dienste (vgl. auch § 15). Dies umfasst insbesondere die Beachtung der informationellen Selbstbestimmung der Betroffenen nach Maßgabe der datenschutzrechtlichen Bestimmungen und die Gewährleistung ausreichender Sicherheit für die über die De-Mail-Dienste verarbeiteten personenbezogenen Daten. Hierzu gehört auch die datenschutzgerechte Gestaltung der Dienste insbesondere durch das Angebot pseudonymer Nutzungsmöglichkeiten der einzelnen Dienste und den Schutz der Pseudonymität. Der Nachweis kann geführt werden durch Vorlage eines vom BfDI erteilten Zertifikates. Das Verfahren könnte sich an bereits bestehenden Regelungen (z. B. des Landes Schleswig-Holstein) orientieren. Als sachverständige Stellen kommen z.B. die vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannten sachverständigen Stellen in Betracht. Bevor der BfDI ein Zertifikat erteilt, muss das vorgelegte Gutachten auf Schlüssigkeit, Zugrundelegung des Kriterienkataloges nach vorletztem Halbsatz sowie auf methodisch einwandfreie Vorgehensweise der sachverständigen Stelle geprüft werden.

Zu Absatz 4

Um akkreditierten Diensteanbietern das Erbringen ihrer Dienste zu erleichtern, wird ihnen ermöglicht, Dritte mit Aufgaben aus diesem Gesetz zu beauftragen. Voraussetzung ist allerdings, dass die Beauftragung des Dritten und deren Umfang in die Konzeption zur Umsetzung der Akkreditierungsvoraussetzungen nach § 18 Absatz 1 aufgenommen wird. Dies gilt insbesondere für die Konzepte zur Gewährleistung von Sicherheit, Funktionalität, Interoperabilität sowie Datenschutz.

Zu § 19 (Gleichstellung ausländischer Dienste)

Zu Absatz 1

Die Vorschrift regelt den Umgang mit ausländischen Angeboten, die den De-Mail-Diensten entsprechen. Die Vorschrift stellt funktional äquivalente Dienste den Diensten akkreditierter Dienstleister gleich, wenn bestimmte Voraussetzungen erfüllt sind. Zum einen müssen die grenzüberschreitenden Dienste eine gleichwertige Vertrauenswürdigkeit bieten, indem sie die den De-Mail-Diensten kennzeichnenden Dienste in vergleichbarer Weise umfassend, zuverlässig, kompatibel, kooperativ und sicher anbieten. Zum anderen muss eine Prüfung und Anerkennung der Vertrauenswürdigkeit durch eine zuständige Stelle des Mitgliedstaats erfolgt sein. Schließlich muss der Mitgliedstaat, in dem der Diensteanbieter seinen Sitz hat, eine gleichwertige Aufsicht bereitstellen. Nur dann kann auf eine Aufsicht im Geltungsbereich dieses Gesetzes verzichtet werden. Die Vorschrift dient der Umsetzung europarechtlicher Anforderungen, insbesondere der künftigen Anforderungen aus den Artikeln 9 ff. DLRL zum Schutz der Niederlassungs- und Dienstleistungsfreiheit. Als Telekommunikations- und Telemediendienste können die Dienste der De-Mail-Dienste elektronisch und damit weitgehend ohne Ortsbezug, also leicht auch grenzüberschreitend, erbracht werden. Die

Regulierung der De-Mail-Dienste hat daher im Rahmen der in der DLRL geregelten Beschränkungen zu erfolgen und darf nicht zu einer Diskriminierung führen. Allerdings betreffen die Anforderungen Dienste von allgemeinem wirtschaftlichem Interesse, die die öffentliche Sicherheit und Ordnung der Bundesrepublik Deutschland berühren. Den Mitgliedstaaten ist daher gestattet, die Erfüllung notwendiger Anforderungen sicherzustellen. Zu vermeiden ist jedoch eine doppelte Prüfung der Dienstleistungserbringer.

Zu Absatz 2

Die Prüfung der Gleichwertigkeit des ausländischen Diensteanbieters obliegt der zuständigen Behörde.

Zur Feststellung der gleichwertigen Sicherheit kann die zuständige Behörde mit der zuständigen ausländischen Stelle die Verfahren zur Anerkennung vereinbaren, soweit nicht entsprechende überstaatliche oder zwischenstaatliche Vereinbarungen getroffen sind.

Die Prüfung der Gleichwertigkeit ist etwas anderes als die Akkreditierung nach § 17. Wird eine Gleichwertigkeit des ausländischen Diensteanbieters angenommen, so wird er damit – anders als bei der Akkreditierung nach § 17 – nicht im Sinne von § 5 Absatz 6 beliehen.

Die zuständige Behörde veröffentlicht die Namen der als gleich vertrauenswürdig anerkannten Dienstleister nach § 22.

Zum Abschnitt 5 (Aufsicht)

Zu § 20 (Aufsichtsmaßnahmen)

Zu Absatz 1

Die Vorschrift weist in Satz 1 der zuständigen Behörde die Aufsicht über akkreditierte Diensteanbieter zu. Das bestehende Regelungssystem der datenschutzrechtlichen Aufsicht bleibt hiervon unberührt.

Die Aufsicht beginnt mit der Akkreditierung (Satz 2). Eine systematische Kontrolle ist nicht vorgesehen; die Aufsicht ist vielmehr auf anlassbezogene Maßnahmen beschränkt.

Zu Absatz 2

Die zuständige Behörde wird in allgemeiner Form ermächtigt, alle geeigneten Maßnahmen und Anordnungen zu treffen, um die Einhaltung der Rechtsvorschriften dieses Gesetzes sicherzustellen. Die hierzu erforderlichen konkreten Befugnisse ergeben sich aus § 21. Die Allgemeinheit dieser Ermächtigung ist erforderlich, um in den nicht voraussehbaren Fällen von Gesetzesverstößen der zuständigen Behörde die notwendigen Möglichkeiten zu eröffnen, die Vorgaben des Gesetzes durchzusetzen. Sie wird im konkreten Fall durch die bewährten Grundsätze des Polizeirechts konkretisiert und begrenzt, insbesondere durch den Grundsatz der Verhältnismäßigkeit. Maßnahmen - etwa durch nachträglichen Erlass einer Nebenbestimmung oder Auflage, soweit dies erfolgversprechend erscheint, um die Einhaltung der Akkreditierungsvoraussetzungen sicherzustellen -, können etwa zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Die Vorschrift ermächtigt nicht nur zu Maßnahmen gegen akkreditierte Diensteanbieter, sondern auch gegen nicht akkreditierte Diensteanbieter, die gegen Vorschriften des Gesetzes verstoßen, weil sie sich etwa als akkreditierte Diensteanbieter ausgeben.

Zu Absatz 3

Die Untersagungsverfügung nach Absatz 3 gibt die Möglichkeit, ein rechtswidriges Verhalten eines akkreditierten Diensteanbieters abzustellen oder zu verhindern. Sie ist für eine befristete Zeit bis zur Beseitigung des rechtswidrigen Verhaltens bestimmt. Eine teilweise Untersagung der Tätigkeit kann z.B. darin bestehen, dass zunächst keine weiteren De-Mail-Konten zugeteilt werden dürfen.

Zu Absatz 4

Die Regelung dient der Klarstellung.

Zu Absatz 5

Mit der Regelung werden der zuständigen Behörde die ihr zur Erfüllung der ihr als Aufsichtsbehörde übertragenen Aufgaben nach Absätzen 1 bis 4 notwendigen prozessualen Eingriffsbefugnisse (Auskunfts-, Betretungs- und Besichtigungsrechte) verliehen. Durch die Worte „in geeigneter Weise“ wird klargestellt, dass die Verpflichtung zur Auskunft und Unterstützung einschließt, dass der akkreditierte Diensteanbieter oder für ihn tätige Dritte der zuständigen Behörde die für die Nutzung elektronischer Daten erforderlichen Einrichtungen zur Verfügung stellen. Durch die Worte „auch soweit sie elektronisch vorliegen“ soll klargestellt werden, dass unter die Aufzählung auch elektronische Dokumente fallen. Dies betrifft jedoch nur solche Dokumente, die die zuständige Behörde als Aufsichtsbehörde zur Erfüllung der ihr als Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, für die Ausübung ihrer Aufsicht benötigt; das betrifft die sich aus diesem Gesetz ergebenden Pflichten der akkreditierten Diensteanbieter. Keinesfalls fallen hierunter z.B. von Nutzern der De-Mail-Dienste bei den akkreditierten Diensteanbietern gespeicherte De-Mails oder sonstige Dokumente.

Zu § 21 (Informationspflicht)

Damit ein EU-weiter Einsatz von De-Mail-Diensten möglich ist, müssen die Nutzer jederzeit online feststellen können, ob es sich bei einem Dienst um einen De-Mail-Dienst handelt, der den Vorschriften dieses Gesetzes oder den entsprechenden nationalen Rechtsvorschriften entspricht. Dies erfordert, dass die jeweilige nationale Aufsichtsstelle ein online abrufbares Verzeichnis der akkreditierten Diensteanbieter oder vergleichbarer ausländischer Diensteanbieter führt. Die Vorschrift ist durch die Wahl des Begriffs „Kommunikationsverbindungen“ technologieoffen gestaltet. Um eine unbemerkte Fälschung oder Verfälschung des Verzeichnisses auszuschließen, muss dieses mit einer qualifizierten elektronischen Signatur signiert sein.

Zum Abschnitt 6 (Schlussbestimmungen)

Zu § 22 (Ausschuss De-Mail-Standardisierung)

Regelungsgegenstand ist die Gründung eines Ausschusses De-Mail-Standardisierung. Aufgabe dieses Ausschusses ist es, bei der Weiterentwicklung der den De-Mail-Diensten zugrundeliegenden technischen Einzelheiten mitzuwirken. Zweck der Vorgabe eines solch formalen Rahmens ist es, dass die Weiterentwicklung in einem – insbesondere für die betroffenen akkreditierten Diensteanbieter – transparenten öffentlichen Prozess erfolgt. Zur Regelung von Einzelheiten über Aufgaben und Verfahren des Ausschusses De-Mail-Standardisierung kann dieser sich eine Geschäftsordnung geben. Das Ergebnis der Arbeit des Ausschusses De-Mail-Standardisierung fließt in die Weiterentwicklung der in der Anlage aufgeführten Technische Richtlinie ein. Dies wird dadurch gewährleistet, dass das BSI nach § 18 Absatz 2 Satz 4 verpflichtet ist, den Ausschuss De-Mail-Standardisierung anzuhören, bevor es wesentliche Änderungen an der Technischen Richtlinie vornimmt.

Zu § 23 (Bußgeldvorschriften)

Die Vorschrift ist erforderlich, um eine wirksame Durchsetzung der gesetzlichen Vorschriften zu ermöglichen. Die Bußgeldvorschrift greift, anders als die zivilrechtliche Haftung, auch

dann, wenn durch das normwidrige Verhalten noch kein Schaden eingetreten oder dies strittig ist.

Ein Bußgeld stellt im Vergleich zu anderen Maßnahmen, die von der zuständigen Behörde im Rahmen ihrer Aufsicht nach § 20 getroffen werden können (z.B. befristete vollständige oder teilweise Untersagung des Betriebes), regelmäßig das mildere und auch flexiblere Mittel zur Durchsetzung der Einhaltung der Vorschriften des Gesetzes und der Verordnung dar. Eine Bußgeldvorschrift ist daher zur Wahrung des allgemeinen Grundsatzes der Verhältnismäßigkeit geboten.

Normadressat der Bußgeldregelung ist der akkreditierte Diensteanbieter. Als Täter einer Ordnungswidrigkeit nach dem Ordnungswidrigkeitengesetz kommt grundsätzlich nur eine natürliche Person in Betracht. In Bezug auf Handlungen von Personen, die für den Normadressaten tätig sind, gilt § 9 Ordnungswidrigkeitengesetz. Die Festsetzung von Bußgeldern gegenüber juristischen Personen regelt § 30 Ordnungswidrigkeitengesetz.

Zu Absatz 1

Absatz 1 enthält die Tatbestände, die erhebliche Auswirkungen auf die Sicherheit von De-Mail-Diensten haben können und denen im Hinblick auf die notwendige Rechtssicherheit bei der Nutzung von De-Mail-Diensten Haftungsregelungen für den Schadensfall allein nicht gerecht werden können.

Zu Nummer 1

Nummern 1 erfasst den Tatbestand, dass der akkreditierte Diensteanbieter die Identität einer Person, die ein De-Mail-Konto beantragt, nicht zuverlässig feststellt. Es handelt sich bei der Identifikation des Antragstellers um eine Kernpflicht des akkreditierten Diensteanbieters. Eine mangelnde Identifikation kann zur Folge haben, dass ein De-Mail-Konto auf einen falschen Namen ausgestellt und dieses für Betrugszwecke eingesetzt wird. Die sichere Identifikation bildet aber einen entscheidenden Baustein für die rechtssichere Kommunikation. Ihr kommt daher im Rechts- und Geschäftsverkehr hohe Bedeutung zu.

Nummer 2

Nummer 2 erfasst den Tatbestand, dass der akkreditierte Dienstanbieter ein Anmeldeverfahren anbietet, das nicht den Anforderungen an die sichere Anmeldung entspricht.

Zu Nummer 3

Nummer 3 erfasst den Tatbestand, dass der Diensteanbieter seinen Lösch-Verpflichtungen nicht ordnungsgemäß nachkommt. In diesen Fällen kann etwa der Nutzer in seinem Recht auf informationelle Selbstbestimmung verletzt sein, wenn etwa seine Identitätsdaten entgegen seines Verlangens vom Diensteanbieter weiter im Verzeichnisdienst veröffentlicht werden.

Zu Nummer 4

Nummer 4 erfasst den Tatbestand, dass der Diensteanbieter seiner Pflicht zur Sperrung des Zugangs zu einem De-Mail-Konto nicht nachkommt. In diesem Fall besteht die Gefahr, dass ein Unbefugter auf das De-Mail-Postfach eines Nutzers zugreifen oder sich unter Missbrauch des Identitätsbestätigungsdienstes im Rechtsverkehr unter der Identität eines bestimmten Nutzers auftreten kann.

Zu Nummer 5

Die Erfüllung der Anzeigepflicht nach § 11 Absatz 1 Satz 1 ist notwendige Voraussetzung dafür, dass die zuständige Behörde ihre Aufsicht nach § 20 wahrnehmen kann.

Zu Nummer 6

Nummer 6 erfasst den Tatbestand, dass ein akkreditierter Diensteanbieter seinen Pflichten bei Einstellung des Betriebes hinsichtlich der Übergabe des De-Mail-Dienstes und der

Sperrung nicht nachkommt. Es geht um die Sicherung der notwendigen Kontinuität der Nutzung sowie um die erforderliche Transparenz im Falle der Einstellung des Betriebes, die für das Vertrauen des Rechts- und Geschäftsverkehrs in die Nutzung von De-Mail-Diensten wichtig ist.

Zu Nummer 7

Nummer 7 erfasst den Tatbestand, dass der akkreditierte Diensteanbieter nicht sicherstellt, dass dem Nutzer für die gesetzlich festgeschriebene Dauer trotz Einstellung seiner Tätigkeit die Möglichkeit des Zugriffs auf das Postfach oder der Dokumentenablage verbleibt. Angesichts der Bedeutung, die De-Mail-Dienste für die rechtssichere Kommunikation im Internet haben können, kann dem Nutzer ein erheblicher wirtschaftlicher und ideeller Schaden entstehen, wenn nicht sichergestellt ist, dass er unabhängig von der Tätigkeit des akkreditierten Diensteanbieters für eine angemessene Zeit den Zugriff auf seine Daten behält.

Zu Nummer 8

Nummer 8 erfasst den Tatbestand, dass der Nutzer nicht im Rahmen der Drei-Monats-Frist auf seine im Postfach oder in der Dokumentenablage abgelegten Daten zugreifen kann. Dies ist etwa dann der Fall, wenn der akkreditierte Diensteanbieter die Daten vor Ablauf der Drei-Monats-Frist löscht. Eine vorzeitige Löschung kann in Anbetracht der Tatsache, dass De-Mail-,Dienste zur rechtssicheren Kommunikation im Internet eingesetzt werden sollen, für den Nutzer einen erheblichen wirtschaftlichen und ideellen Schaden bedeuten. Kann der Nutzer nicht darauf vertrauen, dass seine Daten trotz Vertragsbeendigung für den gesetzlich bestimmten Zeitraum weiter abrufbar sind, kann ihn dies darüber hinaus von einem Anbieterwechsel abhalten. Dies behindert den Wettbewerb unter den verschiedenen akkreditierten Diensteanbietern. Aber auch dann, wenn keine Löschung erfolgt, ist ein umfassender Schutz des Nutzers vor einem Datenverlust nur dann gewährleistet, wenn der akkreditierte Dienstanbieter nicht nur verpflichtet ist, die Daten für einen gesetzlich festgelegten Zeitraum aufzubewahren, sondern dem Nutzer auch die tatsächliche Möglichkeit des Zugriffs auf seine Daten verbleibt. Außerdem erfasst Nummer 8 erfasst den Tatbestand, dass der Nutzer vom akkreditierten Diensteanbieter nicht in geeigneter Weise auf die bevorstehende Löschung hinweist. Dies dient insbesondere dem Verbraucherschutz.

Zu Nummern 9 und 10

Nummer 9 und 10 erfassen die Tatbestände, dass der akkreditierte Diensteanbieter seine Dokumentationspflichten nicht oder nicht vollständig erfüllt. Die Dokumentation ist erforderlich, um nachträglich die Erfüllung der Pflichten des Diensteanbieters überprüfen zu können oder um das Vorliegen der Voraussetzungen einer Akkreditierung kontrollieren zu können. Die Dokumentation kann ein wichtiges Beweismittel sein. Ein Verstoß gegen diese Pflicht untergräbt die zentrale Zielsetzung des Gesetzes, eine nachprüfbare Grundlage für vertrauenswürdige De-Mail-Dienste zu schaffen.

Zu Nummer 11

Nummer 11 berücksichtigt, dass die Akkreditierung eine zentrale Voraussetzung für den sicheren Rechtsverkehr darstellt. Nur aufgrund der Akkreditierung lassen sich an die Nutzung von De-Mail-Diensten bestimmte Rechtsfolgen knüpfen (z.B. Ausstellung der Zugangsbestätigung des Versanddiensts nach § 5 Absatz 8 in Verbindung mit § 5 a Verwaltungszustellungsgesetz (Artikel 3)). Die Akkreditierung als zentraler Vertrauensanker darf daher nicht durch eine missbräuchliche Verwendung der Bezeichnung als akkreditierter Diensteanbieter gefährdet werden.

Zu Absatz 2

Die Vorschrift trägt der Möglichkeit Rechnung, dass ein Verstoß gegen die Tatbestände des Absatzes 1 im Einzelfall von unterschiedlicher Schwere und Bedeutung sein können.

Es liegt im pflichtgemäßen Ermessen der zuständigen Behörde, ob und in welcher Höhe sie im Einzelfall je nach Schwere des Verstoßes gegen die bußgeldbewehrten Vorschriften des Gesetzes eine Geldbuße verhängt (Kann-Bestimmung). Sie kann im Vorfeld einer möglichen Bußgeldverhängung gegenüber dem akkreditierten Diensteanbieter auch nur eine entsprechende Verwarnung aussprechen oder – bei geringeren Verstößen – lediglich auf die Verletzung von Vorschriften hinweisen mit der Bitte, diese abzustellen.

Zu Absatz 3

Diese Vorschrift entspricht den Vorgaben des Gesetzes über Ordnungswidrigkeiten, die eine Benennung der zuständigen Verwaltungsbehörde für die Verfolgung der Ordnungswidrigkeiten verlangt.

Die Zuständigkeit für die Verhängung von Bußgeldern soll bei der zuständigen Behörde nach § 2 liegen. Sie verfügt über die erforderliche Fachkompetenz, um die relevanten Tatbestände entsprechend beurteilen zu können.

Zu § 24 (Gebühren und Auslagen)

Zu Absatz 1
Absatz 1 legt den Kreis der gebühren- und auslagenpflichtigen Amtshandlungen fest. Erfasst sind zunächst Amtshandlungen nach § 17. Dazu gehören die Erteilung der Akkreditierung und des Gütezeichens sowie die Erneuerung der Akkreditierung. Auch können für die Erteilung eines Zertifikates im Sinne von § 18 Absatz 2 Nummer 4 Gebühren verlangt werden. Außerdem kann die Prüfung der Gleichwertigkeit eines ausländischen Diensteanbieters nach § 19 Absatz 2 gebührenpflichtig sein, ebenso die in § 20 Absätze 2 bis 4 geregelten Maßnahmen im Rahmen der Aufsicht. Dazu zählen die Untersagung des Betriebs (§ 20 Absatz 3) oder die Rücknahme oder der Widerruf der Akkreditierung (§ 20 Absatz 4).

Für alle vorgenannten Amtshandlungen ordnet die Vorschrift für die Gebührenbemessung das Kostendeckungsprinzip an. Damit gilt nach § 3 Satz 2 des Verwaltungskostengesetzes das Verbot der Kostenüberdeckung, wonach Gebühren so bemessen sein müssen, dass das geschätzte Gebührenaufkommen den auf die Amtshandlungen entfallenden durchschnittlichen Personal- und Sachaufwand für den betreffenden Verwaltungszweig nicht übersteigt. Die Erhebung von Verwaltungsgebühren zur Erzielung von Überschüssen ist damit nicht gestattet. Bei der Kalkulation der Kosten kann der gesamte auf die einzelnen gebührenpflichtigen Leistungen entfallende Verwaltungsaufwand berücksichtigt werden; dazu zählen auch die durch die Mitwirkung privater Stellen bei der Durchführung der Aufsicht verursachten Kosten, soweit sie den einzelnen Amtshandlungen zurechenbar sind.

Zu Absatz 2
Absatz 2 enthält eine Verordnungsermächtigung zur Ausgestaltung der Regelung über die Gebührenerhebung nach Absatz 1. Nach Satz 2 kann in der Rechtsverordnung auch eine vom Verwaltungskostengesetz abweichende Auslagenerstattung, insbesondere eine Pauschalierung geregelt werden. Nach Satz 3 können Ermäßigungen und Befreiungen von Gebühren und Auslagen nach § 6 des Verwaltungskostengesetzes aus Gründen der Billigkeit oder des öffentlichen Interesses vorgesehen oder zugelassen werden.

Zu Artikel 2 (Änderung der Zivilprozessordnung)
Mit der Regelung werden die ‚De-Mail-Dienste als Übertragungsweg für die Übermittlung elektronischer Dokumente ausdrücklich anerkannt.

Zu Artikel 3 (Änderung des Verwaltungszustellungsgesetzes)

Artikel 3 schafft die Rechtsgrundlage für eine rechtssichere elektronische Zustellung durch die Behörde über De-Mail-Dienste für den Anwendungsbereich des Verwaltungszustellungsgesetzes (VwZG) und passt das bisherige Recht an die neue Rechtslage an. Damit werden die mit dem Vierten Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 11. Dezember 2008 (BGBl. I S. 2418) geschaffenen Vorschriften, die an die heute bestehenden technischen Möglichkeiten der Kommunikation mit E-Mails anknüpfen, fortentwickelt. In diesem Zusammenhang werden auch die Vorschriften über die Zustellung im Ausland im Interesse der Rechtsklarheit modifiziert. Die rechtssichere elektronische Zustellung über De-Mail-Dienste setzt voraus, dass die Behörde sich entschieden hat, Zustellungen über De-Mail-Dienste anzubieten.

Zu Nummer 1

Zu Buchstabe a
Die Änderung ergänzt die nach dem bisherigen § 2 Absatz 2 VwZG abschließend dargestellten Zustellungsarten um die Zustellung über De-Mail-Dienste. Dabei wird der akkreditierte Diensteanbieter nach Artikel 1 § 5 Absatz 6 Satz 2 des De-Mail-Gesetzes als beliehener Unternehmer tätig.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung zu Nummer 2 Buchstabe b.

Zu Nummer 2

Diese Änderung passt die zur Umsetzung der EG-Dienstleistungsrichtlinie erfolgten Änderungen des Verwaltungszustellungsgesetzes (VwZG) an die durch die De-Mail-Infrastruktur ermöglichte verbesserte Beweisführung über den Zugang elektronischer Dokumente an. Danach wird der bisherige § 5 Abs. 7 VwZG dahingehend nachjustiert, dass zur Widerlegung der Zustellungsfiktion das Erfordernis des Vollbeweises an Stelle der Glaubhaftmachung tritt. Die Änderung greift die Stellungnahme des Bundesrates vom 03.04.09 zu Punkt Nr. 21 (BT-Drucksache 16/12598) auf.

Zu Buchstabe a

Die Änderung soll verdeutlichen, dass in dieser Vorschrift auch die elektronische Zustellung geregelt ist, soweit es sich nicht um elektronische Zustellung per Abholbestätigung über De-Mail-Dienste handelt.

Zu Buchstabe b
Die Änderung erfolgt aus Gründen der Rechtsförmlichkeit. Im Interesse einer besseren Zitierbarkeit und einfacheren Verständlichkeit.

Zu Buchstabe c
Mit der Einführung einer rechtssicheren elektronischen Abholbestätigung nach Artikel 1 § 5 Abs. 9 werden die Beweismöglichkeiten über den Zugang bei der elektronischen Zustellung erheblich verbessert. Dementsprechend werden mit der Änderung die in § 5 Abs. 7 Satz 3 VwZG geregelten Beweisanforderungen zur Widerlegung der Zustellungsfiktion gegenüber dem geltenden Recht angehoben: Danach kann der Nachweis der nicht erfolgten oder der verspäteten Zustellung nicht mehr durch Glaubhaftmachung, sondern nur durch einen Vollbeweis seitens des Adressaten erfolgen. Damit übernimmt der Empfänger in Fällen, in denen das Verwaltungsverfahren auf sein Verlangen in elektronischer Form abgewickelt werden muss, die Beweislast für den Nichtzugang oder verspäteten Zugang des elektronischen Dokuments. Auf diese Weise wird der missbräuchlichen Widerlegung der Zustellungsfiktion, z. B. um eine Genehmigungsfiktion eintreten zu lassen, entgegengewirkt.

Nach dem bisherigen § 5 Absatz 7 Satz 4 VwZG hat die zustellende Behörde den Empfänger vor der Übermittlung zu belehren, dass eine Zustellungsfiktion eintritt, wenn er eine elektronische Verfahrensabwicklung verlangt, aber seine Mitwirkung daran verweigert. Mit der Änderung wird die Belehrungspflicht auf das Erfordernis des Vollbeweises zur Widerlegung der Zustellungsfiktion ausgeweitet. Hierdurch wird der Empfänger auf das von ihm zu tragende Risiko einer elektronischen Übermittlung hingewiesen und erhält somit die Möglichkeit, eine andere Form der Zustellung zu wählen.

Zu Nummer 3

Die neu in das VwZG eingefügte Vorschrift ergänzt die bisherigen Möglichkeiten der elektronischen Zustellung nach § 5 Absätze 4 und 5 VwZG. Danach kann die elektronische Zustellung künftig nicht nur im Wege der herkömmlichen E-Mail, sondern auch über De-Mail-Dienste erfolgen. Bei der Zustellung über De-Mail-Dienste wird eine beweissichere elektronische Abholbestätigung eingeführt, die der akkreditierte Diensteanbieter des Empfängers elektronisch erzeugt. Dadurch werden bei der elektronischen Zustellung die Beweismöglichkeiten über den Zugang bzw. die Möglichkeit der Kenntnisnahme erheblich verbessert.

Zu Absatz 1

In Satz 1 wird alternativ zu der bisherigen elektronischen Zustellung per E-Mail nach § 5 Absätze 4 und 5 VwZG die Möglichkeit der förmlichen Zustellung von elektronischen Dokumenten im Anwendungsbereich des Verwaltungszustellungsgesetzes durch Übersendung an das De-Mail-Postfach des Empfängers ermöglicht. Dies gilt sowohl für die obligatorische als auch für die fakultative elektronische Zustellung nach § 5 Absatz 5 Satz 1 VwZG und erfasst auch die Adressaten der vereinfachten Zustellung nach § 5 Absatz 4 VwZG.

Entsprechend der Zielsetzung des Gesetzentwurfs, den elektronischen Rechts- und Geschäftsverkehr zu fördern, knüpft die Verwaltungszustellung über De-Mail-Dienste – ebenso wie die Nutzung von De-Mail-Diensten im Übrigen – an die freiwillige Entscheidung des Nutzers an. Daher ist weder eine rechtliche noch eine faktische Verpflichtung des Empfängers zur Zustellung über De-Mail-Dienste vorgesehen. Dies gilt sowohl für die Anmeldung des Nutzers zum De-Mail-Konto, als auch für die elektronische Zustellung über den De-Mail-Dienst im Einzelfall.

Hat der Nutzer seine De-Mail-Adresse gemäß § 5 Absatz 1 des De-Mail-Gesetzes einer staatlichen Stelle (z. B. im Briefkopf eines an die Behörde gerichteten Schreibens) mitgeteilt, so ist nach der Verkehrsanschauung davon auszugehen, dass der Nutzer dieser Stelle gegenüber einen Zugang im Sinne von § 3a Absatz 1 VwVfG eröffnet und konkludent seinen Willen zum Empfang rechtlich verbindlicher Erklärungen bekundet hat. Hierüber ist der Nutzer bei Eröffnung des De-Mail-Kontos durch den akkreditierten Diensteanbieter nach § 9 des De-Mail-Gesetzes zu informieren. Auf die Begründung zu § 9 Absatz 1 des De-Mail-Gesetzes wird insoweit verwiesen. Die Behörde sollte in diesen Fällen elektronische Zustellungen nach Möglichkeit über die De-Mail-Adresse des Nutzers vornehmen.

Nach Satz 2 gilt bei der Zustellung über De-Mail-Dienste für die Adressaten der vereinfachten Zustellung § 5 Absatz 4 VwZG mit der Maßgabe, dass an die Stelle des Empfangsbekenntnisses die Abholbestätigung tritt; das Gleiche gilt für die in § 5 Absatz 6 VwZG geregelten formellen Anforderungen an die elektronische Zustellung.

Zu Absatz 2

Absatz 2 verpflichtet den akkreditierten Diensteanbieter, eine elektronische Abholbestätigung zu erzeugen und diese der Behörde unverzüglich zu übermitteln. Da die Feststellungen in der elektronischen Abholbestätigung nach Absatz 3 gegenüber dem Richter Bindungswirkung entfalten, handelt der Diensteanbieter bei der Erzeugung der

elektronischen Zugangsbestätigung in Ausübung hoheitlicher Befugnisse. Diese müssen ihm im Wege der Beleihung nach § 5 Absatz 5 Satz 2 des De-Mail-Gesetzes übertragen werden.

Die Normierung der Pflichten des akkreditierten Diensteanbieters im Rahmen der förmlichen Zustellung nach dieser Vorschrift lehnt sich an die Vorschriften über die Postzustellungsurkunde nach § 182 der Zivilprozessordnung an.

Nach Satz 1 ist der akkreditierte Diensteanbieter zur Erzeugung einer elektronischen Abholbestätigung verpflichtet. Diese muss die in § 5 Absatz 9 Satz 4 und 5 des De-Mail-Gesetzes geregelten Anforderungen genügen, um die Zustellung nachweisbar und nachvollziehbar zu machen. Auf die Begründung zu § 5 Absatz 9 Satz 4 des De-Mail-Gesetzes wird insoweit verwiesen.

Nach § 5 Absatz 9 Satz 5 des De-Mail-Gesetzes hat der akkreditierte Diensteanbieter die Abholbestätigung zur Sicherung ihrer Authentizität und Integrität mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

Nach Satz 2 hat der akkreditierte Diensteanbieter die Abholbestätigung unverzüglich nach ihrer Erzeugung an die absendende Behörde zu übermitteln. Dies dient der sicheren Nachweisbarkeit der über das De-Mail-Konto des Empfängers vorgenommenen förmlichen Zustellung durch die Behörde.

Zu Absatz 3

Absatz 3 regelt die Beweiskraft der elektronischen Abholbestätigung. Nach Satz 1 erbringt diese Beweis für die förmliche Zustellung durch die absendende Behörde. Satz 2 stellt hierzu durch den Verweis auf § 371a Absatz 2 der Zivilprozessordnung klar, dass die von einem akkreditierten Diensteanbieter erstellte elektronische Abholbestätigung die Beweiskraft einer öffentlichen Urkunde hat. Damit begründet die elektronische Abholbestätigung nach § 418 der Zivilprozessordnung vollen Beweis für die in ihr bezeugten Tatsachen, die die Mindestinhalte nach § 5 Absatz 9 Satz 4 des De-Mail-Gesetzes umfassen müssen. Mithin erstreckt sich die Beweiskraft darauf, dass die in der Abholbestätigung genannte Nachricht im Zeitpunkt des Anmeldens des Empfängers an seinem De-Mail-Konto im Sinne des Artikel 1 § 4, was zeitlich nach dem Eingang der Nachricht im De-Mail-Postfach des Empfängers liegen muss (daher wird auch der Zeitpunkt des Einlegens der Nachricht in das Postfach der Abholbestätigung angegeben), diesem zugestellt worden ist. Über diese Rechtswirkung der Abholbestätigung wurde der Empfänger auch im Rahmen der Informationspflicht nach Artikel 1 § 9 Absatz 1 durch den akkreditierten Diensteanbieter hingewiesen.

Zu Absatz 4

Die Regelung orientiert sich an § 5 Absatz 7. Sie regelt den Fall der obligatorischen Zustellung über De-Mail-Dienste. Hier wie bei § 5 Absatz 7 gilt, dass das Verlangen nach elektronischer Verfahrensabwicklung als zusätzliche Voraussetzung neben die Zugangserföffnung (hier: über De-Mail-Dienste) tritt. Wird auf Verlangen des Empfängers das Verfahren elektronisch – hier über De-Mail-Dienste – elektronisch abgewickelt, schafft Satz 1 eine Zustellfiktion für die Fälle, in denen der Empfänger sich nicht an seinem De-Mail-Konto anmeldet, so dass keine Abholbestätigung erzeugt werden kann, und dadurch seine Mitwirkung an der Zustellung verweigert. Im Übrigen wird auf die Gesetzesbegründung zu § 5 Absatz 7 (BT-Drucksache 16/10844 vom 12.11.2008) verwiesen.

Zu Nummer 4

Die Änderung des bisherigen § 9 Absatz 1 Nummer 4 VwZG passt die Regelungen über die elektronische Zustellung im Ausland an die durch Nummer 2 geschaffene Ergänzung der bisherigen Zustellungsarten an. Danach kann eine nach Völkerrecht zulässige Zustellung elektronischer Dokumente im und in das Ausland künftig nicht nur im Wege der herkömmlichen E-Mail, sondern auch über De-Mail-Dienste erfolgen.

Zu Buchstabe a

Es handelt sich um eine Folgeänderung zu Nummer 2.

Zu Buchstabe b
Es handelt sich um eine Folgeänderung zu Nummer 2.

Zu Buchstabe c

Die Ergänzung des bisherigen § 9 Absatz 3 VwZG stellt in Anknüpfung an die parallele Vorschrift in § 71b Absatz 6 Satz 3 des Verwaltungsverfahrensgesetzes ausdrücklich auch für die Verwaltungszustellung klar, dass bei einer Verfahrensabwicklung über eine einheitliche Stelle von einem Antragsteller oder Anzeigepflichtigen im Ausland nicht verlangt werden kann, einen Empfangsbevollmächtigten im Inland zu benennen. Durch die ausdrückliche Regelung soll auch bei nichtelektronischen Zustellungsverfahren eine mögliche Benachteiligung ausländischer Antragsteller oder Anzeigepflichtiger ausgeschlossen werden. Dies dient der wirksamen Umsetzung von Artikel 8 Absatz 1 der Dienstleistungsrichtlinie, wonach die Mitgliedstaaten verpflichtet sind, sicherzustellen, dass Verfahren über den einheitlichen Ansprechpartner „problemlos aus der Ferne“ abgewickelt werden können; dies gilt unabhängig davon, ob der Dienstleistungserbringer elektronische Verfahren oder andere Formen von Verfahren wählt.

Zu Artikel 4 (Änderung des Bürgerlichen Gesetzbuches)
Zweck dieser Regelung ist es, ein “Gegenseitigkeitsprinzip“ einzuführen. Die Freiwilligkeit der Nutzung von De-Mail gilt für alle Nutzer: natürliche Personen (also auch in ihrer Eigenschaft als Verbraucher im Sinne von § 13 des Bürgerlichen Gesetzbuches) juristische oder Personengesellschaften (auch in ihrer Eigenschaft als Unternehmer im Sinne von § 14 des Bürgerlichen Gesetzbuches). De-Mail ist umso erfolgreicher, je mehr Nutzer gewonnen werden können. Für die Seite von Unternehmen als „Massenversender“ ergibt sich der Nutzen von De-Mail daraus, dass sie durch Versendung per De-Mail gegenüber der Versendung per herkömmlicher Post Kosten sparen. Für den Bürger ergibt sich der Nutzen daraus, dass sie rechtsgeschäftlich relevanten Schriftverkehr zukünftig elektronisch vornehmen können und dabei nur noch ein De-Mail-Konto benötigen. Verbraucher müssen also z. B. nicht mehr Web-Portale der verschiedenen Unternehmen nutzen. Voraussetzung hierfür ist allerdings, dass die Betreiber dieser Web-Portale, in der Regel Unternehmer, „Massenversender“, ihre Kunden, die sie per De-Mail erreichen können, nicht wieder auf ihre Portale verweisen, sondern die De-Mail-Nachrichten ihrer Kunden entgegennehmen. Dass es diese Alternative überhaupt gibt, ergibt sich daraus, dass das Erfordernis der „Textform“ nach § 126b BGB sowohl durch eine übersandte E-Mail als auch durch das tatsächliche Downloaden von Dokumenten auf Web-Portalen seitens des Empfängers gewahrt ist (vgl. Palandt, Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, Rn. 3 zu § 126b). Auf ihrem De-Mail-Konto können Bürger als Verbraucher rechtsgeschäftlich relevante Kommunikation empfangen (dies ist das Interesse der „Massenversender“) aber auch versenden (dies ist das Interesse der natürlichen Person als Verbraucher, Kunde eines Massenversenders). Um eine rasche Akzeptanz beim Bürger zu erreichen, sollten im Sinne einen Gegenseitigkeitsprinzips Unternehmen verpflichtet werden, dass sie, wenn sie mit ihren Kunden per De-Mail kommunizieren, genauso den Empfang von De-Mail-Nachrichten ihrer Kunden akzeptieren. Der Erreichung dieses Zieles dient die vorgeschlagene Änderung von § 312e des Bürgerlichen Gesetzbuches.

Zu Artikel 5 (Evaluierung)
Die Bundesregierung beobachtet die Entwicklung der De-Mail-Dienste und legt dar, ob und gegebenenfalls in welchen Bereichen Anpassungs- oder Ergänzungsbedarf bei den rechtlichen Rahmenbedingungen für die neuen Dienste und bei den Vorschriften über die elektronische Zustellung besteht. Hierbei wird sie insbesondere auch prüfen, ob die Einführung einer Zertifizierung von Verbraucherschutzkriterien als Voraussetzung für die Akkreditierung von Diensteanbietern geboten ist. Bei der Evaluierung der Vorschriften über die elektronische Zustellung soll insbesondere geprüft werden, ob diese den Erfordernissen der Verwaltungspraxis hinreichend gerecht werden. Auch sollten die Akzeptanz, Effizienz und Anwendungstiefe des De-Mail-Dienstes Berücksichtigung finden. Die Bundesregierung

legt hierüber dem Deutschen Bundestag bei Bedarf, spätestens jedoch nach Ablauf von drei Jahren nach Inkrafttreten dieses Gesetzes einen Bericht vor.

Zu Artikel 6 (Inkrafttreten)

Artikel 6 regelt das Inkrafttreten des Gesetzes.