Erläuterungen

I. Allgemeiner Teil

Mit der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates wurden Regelungen zu elektronischen Signaturen festgelegt, ohne aber einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die Richtlinie 1999/93/EG beschränkte sich vielmehr auf den Bereich elektronischer Signaturen, wobei die Umsetzungs- und Anwendungspraxis der Mitgliedstaaten auch dort einige Defizite zeigten. Der Bereich der elektronischen Identifizierung blieb bislang unionsrechtlich ungeregelt, auch eine gegenseitige Anerkennung der national etablierten elektronischen Identifizierungsmethoden fehlte bisher.

Mit der Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257/73 vom 28. August 2014 (so genannte „eIDAS-VO“) sollen nunmehr ua die Rechtsvorschriften jener Richtlinie gestärkt und erweitert werden, indem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen geschaffen wird. Dadurch wird die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht. Zudem wird der Bereich der elektronischen Identifizierung angesprochen.

Die eIDAS-VO regelt somit im Wesentlichen zwei Themenkreise:

1. Vertrauensdienste

Das sind elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, Zustellung elektronischer Einschreiben, Website-Authentifizierung und Validierungs- sowie Bewahrungsdienste.

2. Elektronische Identifizierung

Dabei werden Bedingungen festgelegt, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anzuerkennen haben.

Die Durchführung der unmittelbar anwendbaren eIDAS-VO erfordert eine Anpassung jener innerstaatlichen Gesetze, die die Themen elektronische Identifizierung (E-GovG) bzw. elektronische Signaturen (SigG) derzeit regeln, wobei anstelle des aufzuhebenden SigG ein neues Signatur- und Vertrauensdienstegesetz (SVG) erlassen werden soll.

Zu Artikel 1 (Signatur- und Vertrauensdienstegesetz – SVG)

Durch die Schaffung eines EU-weit harmonisierten Rechtsrahmens für Vertrauensdienste soll das Signaturgesetz aufgehoben werden und für das Thema Vertrauensdienste ein neues Begleit- bzw. Durchführungsgesetz zur eIDAS-VO erlassen werden.

Im SVG werden nur jene Bereiche geregelt in denen die unmittelbar anwendbare eIDAS-VO den Mitgliedstaaten die Möglichkeit überlässt, nationale Vorschriften zu erlassen. Dies betrifft insbesondere Regelungen bzw. Konkretisierungen in den Bereichen der Vertrauensdiensteanbieter, Aufsicht, Formvorschriften, Haftung und Sanktionen bei Nichteinhaltung der Vorgaben der eIDAS-VO.

Obwohl sich der vorliegende Entwurf auf alle Vertrauensdienste gleichermaßen bezieht, bilden die Erstellung, Validierung und Bewahrung elektronischer Signaturen den Kern, weshalb auch Regelungen des aufzuhebenden SigG im Mittelpunkt sind. Darauf soll auch im Gesetzestitel durch die gesonderte Nennung elektronischer Signaturen ausdrücklich hingewiesen werden

Die Hauptgesichtspunkte sind:

- Beibehaltung der bisher nach dem SigG geltenden Rechtswirkungen der Schriftlichkeit iSd § 886 ABGB einer qualifizierten elektronischen Signatur in Hinblick auf allgemeine Formvorschriften des österreichischen Zivilrechts;
- Nutzer von elektronischen Signaturen sollen auf die Wirksamkeit ihrer qualifiziert elektronisch signierten Dokumente vertrauen können. „Versteckte“ Klauseln in Allgemeinen Geschäftsbedingungen, die dies insbesondere für Vertragskündigungen gegenüber Konsumenten ausschließen, sollen beseitigt werden.
- Pflichten von Signatoren und Siegelerstellern hinsichtlich der sorgfältigen Verwahrung der Signatur- und Siegelerstellungsdaten;
- Vorläufige Aussetzungsmöglichkeit eines qualifizierten Zertifikats wegen bestimmter Gründe;

- Ausstellung qualifizierter Zertifikate durch einen Vertrauensdiensteanbieter;
- Haftungsregelungen, Vertrauensinfrastruktur und Beendigungsplan für Vertrauensdiensteanbieter;
- Festlegung der Telekom-Control-Kommission als Aufsichtsstelle über Vertrauensdiensteanbieter;
- Festlegung der Führung der Vertrauensliste bzw. eines Prüfservices durch die RTR-GmbH;
- Verordnungsermächtigung des Bundeskanzlers für die Benennung einer Bestätigungsstelle.

Zu Artikel 2 (Änderung des E-Government-Gesetzes)

Die eIDAS-Verordnung harmonisiert nicht die bereits in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme und zugehörige Infrastrukturen, sondern schafft den Rechtsrahmen zur gegenseitigen Anerkennung der verschiedenen elektronischen Identifizierungsmittel unter bestimmten normierten Voraussetzungen. Durch eine gegenseitige Anerkennung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten zumindest die Authentifizierung für öffentliche Dienste ermöglichen, soll die grenzüberschreitende Erbringung von Dienstleistungen im Binnenmarkt deutlich erleichtert und der „digitale Binnenmarkt“ insgesamt gestärkt werden. Das bewährte System der österreichischen Bürgerkarte insbesondere in ihrer Ausprägung als Handy-Signatur, wird somit grundsätzlich bestehen bleiben und erfährt im Hinblick auf die künftige rechtliche Anerkennung in den anderen EU-Mitgliedstaaten eine deutliche Ausweitung ihrer Einsatzmöglichkeiten. Die legistischen Anpassungen in Hinblick auf die Interoperabilität der österreichischen Lösung, aber auch um elektronische Identifizierungsmittel anderer Mitgliedstaaten in Österreich anerkennen zu können, sind aber nicht Teil der vorliegenden Novelle und sollen zeitnahe in einem gesonderten legistischen Vorhaben vorgenommen werden.

Mit der gegenständlichen Novelle werden im E-GovG zunächst lediglich jene Bestimmungen geändert, die zur Durchführung der eIDAS-VO unerlässlich sind. Weiters wird der technischen Weiterentwicklung Rechnung getragen und an einigen Stellen im Gesetz eine Klarstellung vorgenommen. Durch eine verstärkte Nutzung von Registerdaten sollen Bürger und Unternehmen stärker entlastet werden.

Zu Artikel 3 bis Artikel 26

Aufgrund der Aufhebung des SigG sollen sämtliche Bestimmungen in Bundesgesetzen, die bisher auf das SigG verwiesen haben, nunmehr auf die entsprechenden Bestimmungen der eIDAS-VO bzw. des SVG verweisen. In jenen Fällen in denen im SVG keine Nachfolgebestimmung zum SigG erlassen werden soll bzw. die eIDAS-VO keine Nachfolgeregelung vorsieht, sollen entsprechende Streichungen in den Bundesgesetzen vorgenommen werden. Dabei sollen keine sonstigen inhaltlichen Änderungen vorgenommen werden.

Zuständigkeit des Bundes

Die Zuständigkeit des Bundes zur Gesetzgebung und Vollziehung beruht auf den Kompetenztatbeständen „Zivilrechtswesen“ gemäß Art. 10 Abs. 1 Z 6 B-VG, „Angelegenheiten des Gewerbes und der Industrie“ gemäß Art. 10 Abs. 1 Z 8 B-VG, „Post- und Fernmeldewesens“ gemäß Art. 10 Abs. 1 Z 9 B-VG, „Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr“ gemäß § 2 des Datenschutzgesetzes 2000, weiters auf die Bedarfsgesetzgebungskompetenz für das Verwaltungsverfahren nach Art. 11 Abs. 2 B-VG, „Meldewesen“ gemäß Art. 10 Abs. 1 Z 7 B-VG, „Verfassungsgerichtsbarkeit“ gemäß Art. 10 Abs. 1 Z 1 B-VG und „Einrichtung der Bundesbehörden …“ gemäß Art. 10 Abs. 1 Z 16 B-VG.

II. Besonderer Teil

Zu Artikel 1 (Signatur- und Vertrauensdienstegesetz – SVG)

Zu § 1:

Die eIDAS-VO ist auf Grund ihres Rechtscharakters in allen Mitgliedstaaten unmittelbar anwendbar und besitzt allgemeine Geltung. Dennoch enthält die Verordnung einzelne Artikel, die den Mitgliedstaaten Regelungskompetenzen im nationalen Recht überlassen oder sogar vorschreiben. Mit dem Signatur- und Vertrauensdienstegesetz (SVG) sollen die notwendigen Durchführungs- und Begleitbestimmungen zu den Bestimmungen der eIDAS-VO, die Vertrauensdienste und Vertrauensdiensteanbieter betreffen, erlassen werden. Nicht Regelungsgegenstand dieses Gesetzes sind die Vorschriften des Kapitels II der eIDAS-VO über die elektronische Identifizierung, da dieser Bereich bereits im E-Government-Gesetz (und seinen VOen), geregelt ist und dieses daher gesondert zu novellieren ist.

Das SVG tritt an die Stelle des Signaturgesetzes (SigG), mit dem in Österreich die Signaturrichtlinie (RL 1999/93/EG) umgesetzt wurde und welche durch die eIDAS-VO mit 1.7.2016 aufgehoben wird. Der Anwendungsbereich ist aber nunmehr im Sinne der eIDAS-VO weiter gefasst und beschränkt sich nicht mehr ausschließlich auf Regelungen zu elektronischen Signaturen. Vielmehr sind die Erstellung, Überprüfung und Validierung von elektronischen Signaturen nur ein Teil der Vertrauensdienste nach der eIDAS-VO. Darüber hinaus sind etwa noch die Erstellung, Überprüfung und Validierung elektronischer Siegel oder von Zertifikaten für Website-Authentifizierung und Dienste für die Zustellung elektronischer Einschreiben erfasst. Die Aufzählung der Vertrauensdienste in § 1 ändert in keiner Weise den Anwendungsbereich oder die Definition der Vertrauensdienste gemäß Art. 3 Z 16 der eIDAS-VO, sondern dient lediglich dem besseren Verständnis bei der Lektüre des SVG.

Zu § 2:

Im Sinne der besseren Lesbarkeit wird auf ein durchgängiges Gendern im Gesetz verzichtet und auf eine Generalklausel zurückgegriffen.

Zu § 3:

Die Begriffsbestimmungen des Abs. 1 sollen der Festlegung sprachlicher Anpassungen und Abkürzungen dienen und eine bessere Lesbarkeit und Übersichtlichkeit des Gesetzes bewirken. Mit dem Begriff „eIDAS-VO“ in Z 1 wird die nicht-amtliche Abkürzung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, die sich aber in der Praxis EU-weit in den allgemeinen Sprachgebrauch eingebürgert hat, verwendet und für die Zwecke der Durchführungsmaßnahmen in der österreichischen Rechtsordnung normiert.

Signatoren gemäß Z 3 sind natürliche Personen, die eine elektronische Signatur erstellen. Die deutsche Fassung der eIDAS-VO bezeichnet diese Personen als „Unterzeichner“, was jedoch keine klare Abgrenzung zwischen Personen, die (Papier)Dokumente handschriftlich unterzeichnen bzw. unterschreiben und jenen, die elektronisch signieren, zulässt und somit in der Praxis zu Missverständnissen führen kann. Um diesem Problem vorzubeugen und auch die bewährte Verwendung des Begriffs „Signator“ nach der Aufhebung des SigG weiterzuführen, erscheint hier eine Abweichung von der Begriffsbestimmung der eIDAS-VO sinnvoll.

Ebenso soll auch die Bezeichnung „Bestätigungsstelle“ aus dem SigG weitergeführt werden.

Darüber hinaus sind gemäß Abs. 2 die Begriffsbestimmungen des Art. 3 eIDAS-VO maßgeblich.

Zu § 4:

Nach Artikel 25 Abs. 2 der eIDAS-VO hat eine qualifizierte elektronische Signatur die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Im Vergleich zu § 4 Abs. 1 des mit Inkrafttreten dieses Gesetzes aufgehobenen Signaturgesetzes ergibt sich diese Rechtswirkung nunmehr bereits aus der eIDAS-VO und braucht daher in Abs. 1 nicht mehr wiederholt zu werden. In Zusammenschau mit Artikel 2 Abs. 3 der eIDAS-VO, wonach die Verordnung nicht das nationale Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige Formvorschriften berührt, bedeutet dies, dass einer qualifizierten elektronischen Signatur zwar die gleiche Rechtswirkung wie einer handschriftlichen Unterschrift zukommt, aber sowohl im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen als auch im Zusammenhang mit anderen rechtlichen Verpflichtungen die zwingende Einhaltung besonderer Formvorschriften durch Gesetz oder durch Parteienvereinbarung vorgesehen werden kann.

Es wird daher weiterhin wie in § 4 Abs. 1 des mit Inkrafttreten dieses Gesetzes aufgehobenen Signaturgesetzes in Abs. 1 angeordnet, dass eine qualifizierte elektronische Signatur das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB erfüllt. Andere gesetzliche oder vertragliche Formerfordernisse, insbesondere solche, die die Beiziehung eines Notars oder eines Rechtsanwalts oder auch eine gerichtliche Tätigkeit vorsehen, sollen aber unberührt bleiben. In diesem Sinne werden in Abs. 2 besondere Formerfordernisse für bestimmte Arten von Willenserklärungen normiert und in Abs. 3 die Privatautonomie im Verhältnis zwischen Unternehmern und Verbrauchern im Interesse der Verbraucher eingeschränkt.

Im österreichischen Zivilrecht werden die Wirkung und das Erfordernis der Schriftform in § 886 ABGB geregelt. Ist für einen Vertrag gesetzlich oder aufgrund einer Parteienvereinbarung das Erfordernis der Schriftlichkeit vorgesehen, so kommt ein Vertrag durch die Unterschrift der Parteien zustande. Der schriftliche Abschluss des Vertrages kann durch die gerichtliche oder notarielle Beurkundung ersetzt werden. Eine Nachbildung der eigenhändigen Unterschrift auf mechanischem Weg ist nur dann ausreichend, wenn dies im Geschäftsverkehr üblich ist.

Vielfach verlangen zivilrechtliche Rechtsvorschriften für die Gültigkeit eines Rechtsgeschäfts die Einhaltung der (einfachen) Schriftform im Sinne des § 886 ABGB. Dies gilt beispielsweise für die Abgabe einer Bürgschaftserklärung durch Personen die nicht Unternehmer iSd UGB sind (§ 1346 Abs. 2 ABGB), die Begründung von Wohnungseigentum (§ 3 Abs. 1 Z 1 WEG), den Abschluss eines befristeten Mietvertrages (§ 29 Abs. 1 Z 3 MRG), den Bauträgervertrag (§ 3 Abs. 1 BTVG), bestimmte Regelungen im Maklervertrag (§ 31 KSchG), die Anerkennung eines bis dahin schwebend unwirksamen Vertrages durch den volljährig Gewordenen (§ 168 ABGB), die Annahme an Kindes statt (§ 192 ABGB), eine Schenkung ohne wirkliche Übergabe (§ 943 ABGB), Verträge über Leistungen zur Sanierung von Wohnräumen (§ 26d KSchG) oder den Heimvertrag (§ 27d Abs. 5 KSchG).

Die Nichtbeachtung gesetzlicher Formvorschriften hat die Ungültigkeit des Rechtsgeschäfts zur Folge. Soweit durch das formungültige Rechtsgeschäft eine Leistungsverpflichtung des Schuldners herbeigeführt werden sollte, wird grundsätzlich eine Naturalobligation erzeugt, also eine Leistungsverbindlichkeit, die zwar nicht vor Gericht durchsetzbar, aber erfüllbar ist. Die tatsächliche Leistung des Versprochenen heilt den Mangel der Form.

Auch bei vertraglich vereinbarten Formvorschriften wird vermutet, dass die Einhaltung dieser Form ein Gültigkeitserfordernis für das Rechtsgeschäft darstellen soll (§ 884 ABGB). Diese Vermutung kann jedoch bei gegenteiligem Willen der Parteien von ihnen entkräftet werden.

Wie bereits ausgeführt, wird das sich entweder aus dem Gesetz oder aus der Parteienvereinbarung ergebende Erfordernis der „Schriftlichkeit“ im Prinzip durch die eigenhändige Unterschrift des Erklärenden erfüllt. Für das wirksame Zustandekommen eines formgebundenen Vertrags ist somit die Unterschrift der Parteien maßgeblich. Gemäß Absatz 1 erfüllt auch eine qualifizierte elektronische Signatur dieses Formerfordernis und können daher mit einer qualifizierten elektronischen Signatur sowohl gesetzlichen, als auch vertraglich vereinbarten Schriftformerfordernissen Genüge getan werden.

Durch Parteienvereinbarung oder Gesetz können aber auch andere Formerfordernisse vorgesehen werden.

So bleibt es Vertragsparteien unbenommen, im Sinne einer besonderen Formvorschrift zu vereinbaren, dass im Geschäftsverkehr zwischen ihnen die Schriftform nicht mittels einer qualifizierten elektronischen Signatur oder bereits bei Verwendung anderer elektronischer Mittel (z. B. E-Mail) gegeben ist.

Besondere gesetzliche Formerfordernisse werden in Abs. 2 normiert. In Anlehnung an den Ausnahmekatalog des § 4 Abs. 2 des mit Inkrafttreten dieses Gesetzes aufgehobenen Signaturgesetzes wird geregelt, dass letztwillige Verfügungen (in Anpassung an die Terminologie des Erbrechtsänderungsgesetzes 2015 statt „Anordnungen“) in elektronischer Form nicht wirksam errichtet werden können und dass Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind, sowie eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird, nur dann in elektronischer Form wirksam abgefasst werden können, wenn das Dokument über die Erklärung die Erklärung eines Notars oder eines Rechtsanwalts enthält, dass er den Signator über die Rechtsfolgen seiner Signatur aufgeklärt hat. Willenserklärungen des Familien- und Erbrechts und eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird, werden somit nur dann der elektronischen Form geöffnet, wenn ein Notar oder ein Rechtsanwalt am Zustandekommen der Erklärung beratend beteiligt war und eine entsprechende Erklärung auch mit seiner Berufssignatur dokumentiert. Explizit ausgenommen soll aber auch weiterhin die Errichtung letztwilliger Anordnungen in elektronischer Form bleiben.

Die besonderen Formerfordernisse für Willenserklärungen des Familien- und Erbrechts sind deshalb gerechtfertigt, weil diese Bereiche besonders sensibel sind, häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen und der Beweis hier vielfach nur schwer erbracht werden kann. Darüber hinaus besteht gerade im Bereich des Familien- und Erbrechts eine größere Missbrauchsgefahr durch die Weitergabe oder das Ausspähen von Autorisierungscodes (z. B. Pin-Code). Dem gegenüber ist etwa eine Unterhaltsverpflichtungserklärung eines – gesetzlich zum Unterhalt verpflichteten – Elternteils nicht als formgebundenes Rechtsgeschäfts zu qualifizieren, sie kann daher auch in elektronisch signierter Form abgegeben werden.

Weil Bürgschaften für den Bürgen in der Regel mit einem beträchtlichen Risiko verbunden sind, ist auch das besondere Formerfordernis für eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird, sachlich gerechtfertigt.

Keinesfalls aber sollte der Rechtsverkehr über das unbedingt Notwendige hinaus mit besonderen Formvorschriften belastet werden. Aus Gründen der Rechtsklarheit und mangels eines erkennbaren

Anwendungsbereichs in der Praxis sieht der Entwurf daher davon ab, weitere besondere Formerfordernisse für die im Ausnahmekatalog des § 4 Abs. 2 des Signaturgesetzes auch enthaltenen Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind (Z 2) sowie Willenserklärungen, Rechtsgeschäfte oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen (Z 3) zu schaffen. Das ändert aber nichts daran, dass vertraglich oder gesetzlich bestimmte Formerfordernisse zur Wirksamkeit einer Erklärung oder eines Rechtsgeschäfts nach wie vor beispielsweise einen Notariatsakt oder eine gerichtliche oder notarielle Beglaubigung verlangen (vgl. Abs. 1 zweiter Satz).

Die Bestimmung des Absatzes 3 dient der Sicherung der gerechtfertigten Erwartungshaltung von Verbrauchern. In der Anwendungspraxis der letzten Jahre wurde in einer Vielzahl von Fällen von gleichsam „versteckten“ Klauseln in Allgemeinen Geschäftsbedingungen berichtet, die insbesondere für Vertragskündigungen die Wirksamkeit qualifiziert elektronisch signierter Dokumente von Verbrauchern ausgeschlossen hatten, obwohl beispielsweise bei Vertragsabschlüssen oder sonstiger Korrespondenz mit den betreffenden Unternehmen die qualifizierte elektronische Signatur von diesen Unternehmen problemlos akzeptiert wurde. Aus Sicht der Verbraucher ist daher im – mittlerweile üblichen – elektronischen Verkehr mit Unternehmen nicht zu erwarten, dass ein Unternehmen ein qualifiziert elektronisch signiertes Dokument als nicht wirksam erachtet. Im Sinne der Privatautonomie soll der Ausschluss der Wirksamkeit qualifiziert elektronisch signierter Dokumente auch im Vertragsverhältnis zwischen einem Unternehmer und einem Verbraucher grundsätzlich weiterhin möglich sein, ein derartiger Ausschluss soll aber im Interesse der Transparenz für die Verbraucher ausdrücklich und einzeln zu vereinbaren sein und somit in Allgemeinen Geschäftsbedingungen nicht wirksam vereinbart werden können.

Die Übernahme des § 4 Abs. 3 des mit Inkrafttreten dieses Gesetzes aufgehobenen Signaturgesetzes in das SVG erübrigt sich, da § 294 ZPO in der Fassung BGBl I 2005/164 (BRÄG 2006) die Möglichkeit der elektronischen Errichtung von Privaturkunden bereits berücksichtigt.

Zu § 5:

Um Missbräuche zu vermeiden, treffen Signatoren und Siegelersteller oder von ihnen dazu beauftragte qualifizierte VDA (im Falle von sogenannten Fernsignaturen; vgl. dazu Anhang II (3) und Erwägungsgrund Nr. 52 der eIDAS-VO) im Umgang mit Signaturerstellungsdaten für qualifizierte elektronische Signaturen bzw. Siegelerstellungsdaten für qualifizierte elektronische Siegel gewisse Pflichten. Elektronische Signaturerstellungs- bzw. Siegelerstellungsdaten sind eindeutige Daten, wie private Signaturschlüssel, die vom Signator oder Siegelersteller zum Erstellen einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden. Der Signator und der Siegelersteller oder von ihnen dazu beauftragte qualifizierte VDA haben diese sorgfältig zu verwahren, unbefugte Zugriffe darauf zu verhindern und deren Weitergabe zu unterlassen. Die Weitergabe von elektronischen Siegelerstellungsdaten soll an autorisierte Personen, in der Regel natürliche Personen die eine juristische Person vertreten, jedoch zulässig sein, da ein Handeln einer juristischen Person sonst nicht möglich wäre.

Bei Verlust oder Kompromittierung (z. B. Verdacht des Ausspähens eines PIN-Codes oder Unmöglichkeit der Rücknahme von elektronischen Siegelerstellungsdaten von nicht mehr autorisierten Personen) der elektronische Signaturerstellungs- bzw. Siegelerstellungsdaten hat der Signator bzw. Siegelersteller den Widerruf des qualifizierten Zertifikats zu verlangen. Dies gilt ebenso, wenn sich sein Name oder andere im qualifizierten Zertifikat bescheinigte Umstände (z. B. von Berufsverbänden oder Kammern bestätigte Eigenschaften) ändern.

Zu § 6:

Aufgrund der Regelungen des Art. 28 Abs. 5 bzw. Art. 38 Abs. 5 eIDAS-VO ist es den Mitgliedstaaten überlassen, nationale Vorschriften zur vorläufigen Aussetzung eines qualifizierten Zertifikats für eine elektronische Signatur oder ein elektronisches Siegel zu erlassen. In § 6 soll von dieser Möglichkeit Gebrauch gemacht und die Gründe für die vorläufige Aussetzung von qualifizierten Zertifikaten geregelt werden. Während ein Widerruf die vorzeitige Beendigung der Gültigkeit eines Zertifikats darstellt, ist eine Aussetzung als vorübergehendes Aussetzen der Gültigkeit eines Zertifikats zu verstehen. Wann ein qualifiziertes Zertifikat zu widerrufen ist, ergibt sich aus der eIDAS-VO, insb. Art. 24 Abs. 3. Besondere Regelungen zum Widerruf bei Einstellung der Tätigkeit enthält § 9.

§ 6 Abs. 1 Z 1 (Aussetzung auf Verlangen des Signators, des Siegelerstellers oder eines sonstigen dazu Berechtigten) ist notwendig, um bei Verdacht auf Verlust oder Kompromittierung der Signaturerstellungsdaten einen möglichen Missbrauch zu verhindern. Enthält ein Zertifikat zusätzliche Attribute, etwa das Bestehen einer berufsrechtlichen oder sonstigen Qualifikation, so kann – wenn sich

hinsichtlich dieser Angaben Änderungen ergeben – auch ein sonstiger dazu Berechtigter die Aussetzung verlangen. Eine solche Berechtigung könnte im Einzelfall etwa einer Berufsvertretung oder einem Dienstgeber zukommen. Weitergehende vertragliche Vereinbarungen, nach denen auch andere Personen eine Aussetzung veranlassen können, bleiben unberührt.

Die Aufsichtsstelle hat – als Aufsichtsmittel – nicht nur die Möglichkeit, einem qualifizierten VDA den Qualifikationsstatus zu entziehen, sie kann die Aussetzung (bzw. den Widerruf gem. Art. 24 Abs. 3 eIDAS-VO) von Anwender-Zertifikaten auch gegenüber dem VDA anordnen (Z 2).

Die Angaben, die in einem qualifizierten Zertifikat bescheinigt werden können, sind grundsätzlich nicht beschränkt (Art. 28 Abs. 3 und Art. 38 Abs. 3 eIDAS-VO). Es können daher zusätzlich fakultative spezifische Attribute enthalten sein, sofern diese die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen oder Siegel nicht berühren. Es muss nur die Zustimmung des Signators oder des Siegelerstellers, gegebenenfalls auch einer dritten Person vorliegen. Bei sonstigen Änderungen im Zertifikat bescheinigter Angaben (Z 3) kann es sich somit um die verschiedensten Umstände handeln, etwa den Entzug einer behördlichen oder berufsrechtlichen Befugnis (siehe dazu auch die Ausführungen zu Z 1) oder einer sonstigen Zulassung.

Die Gefahr einer missbräuchlichen Verwendung (Z 5) besteht etwa bei Verlust oder Kompromittierung des Signaturschlüssels, wenn Signaturschlüssel im Zusammenhang mit Straftaten verwendet werden oder wenn das eingesetzte kryptographische Verfahren nach dem Stand der Technik unsicher wird.

§ 6 Abs. 2 entspricht den Vorgaben der eIDAS-VO zum Widerruf von qualifizierten Zertifikaten und soll daher auch für die Aussetzung gelten.

Gemäß Art. 28 Abs. 5 und Art. 38 Abs. 5 eIDAS-VO können nationale Vorschriften zur vorläufigen Aussetzung eines qualifizierten Zertifikats nur vorbehaltlich der in diesen Bestimmung genannten Bedingungen erlassen werden. Diese wurden daher in die nationale Regelung in Abs. 3 und Abs. 4 aufgenommen.

Wurde eine Aussetzung nicht innerhalb des Zeitraums von zwei Wochen aufgehoben, so ist das qualifizierte Zertifikat zu widerrufen. Wurde die Aussetzung aufgehoben, bedeutet dies für die Gültigkeit des Zertifikats, dass dieses ohne zeitliche Unterbrechung immer gültig war. Dies ergibt sich schon aus der Formulierung der eIDAS-VO (vgl. Art. 28 Abs. 5 lit. a und b sowie Art. 38 Abs. 5 lit. a und b), wonach das Zertifikat „für die Dauer der Aussetzung seine Gültigkeit“ verliert und der Status der Aussetzung wiederum (lediglich) „während der Dauer der Aussetzung“ ersichtlich ist.

Zu § 7:

Zur Gewährleistung der Sicherheit elektronischer Signaturverfahren kommt der Vertrauenswürdigkeit und fachlichen Kompetenz einer Bestätigungsstelle entscheidende Bedeutung zu. Entsprechend der Bestimmung des Art. 30 Abs. 1 der eIDAS-VO kann mit den Aufgaben der zu benennenden Stelle nur eine geeignete Einrichtung betraut werden. Diese gem. Art. 30 Abs. 2 vom Mitgliedstaat der EU-Kommission zu benennenden Stellen sollen in Österreich (weiterhin) die Bezeichnung Bestätigungsstelle tragen.

In § 7 Abs. 1 werden die Kriterien der Eignung einer Bestätigungsstelle näher umschrieben. Im Besonderen wird ausdrücklich festgehalten, dass eine derartige Einrichtung über die erforderlichen Fachkenntnisse und technischen Mittel verfügen sowie Unabhängigkeit und Objektivität gewährleisten muss. Das Kriterium der erforderlichen Zuverlässigkeit sowie des zuverlässigen Personals entspricht der geltenden Rechtslage und hat sich bewährt. Da sich die Beurteilung der Sicherheitsanforderungen nach dem jeweiligen Stand der Technik zu richten hat, muss auch eine laufende Technologiebeobachtung stattfinden.

In Art. 30 Abs. 4 der eIDAS-VO ist vorgesehen, dass die besonderen Kriterien für die Eignung einer in Abs. 1 dieses Artikels angeführten benannten Stelle mittels von der EU-Kommission zu erlassender delegierter Rechtsakte festgelegt werden können. Sobald solche harmonisierten Kriterien vorliegen, muss sich die Beurteilung der Eignung einer solchen Stelle nach diesen Kriterien richten.

§ 7 Abs. 2 enthält die Verordnungsermächtigung zur Benennung von Bestätigungsstellen. Für eine solche Benennung muss die Einhaltung der maßgeblichen Kriterien nachgewiesen sein. Gegenwärtig besteht eine solche Bestätigungsstelle aufgrund der Verordnung über die Feststellung der Eignung des Vereins„Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ als Bestätigungsstelle, BGBl. II Nr. 31/2000.

Die Bestätigungsstelle zertifiziert die Konformität qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten mit den Anforderungen des Anhangs II der eIDAS-VO. Das heißt sie hat vor allem die Einhaltung der vorgeschriebenen Sicherheitsanforderungen durch Signaturprodukte und

Verfahren (technische Komponenten) zu beurteilen und durch ihre Expertise zu objektivieren. Insbesondere bei der Verwendung von Chipkartentechnologien oder Technologien für Sicherheitsmodule müssen zur Vornahme dieser Beurteilungen in der Regel technische Prüfergebnisse zur Verfügung stehen, die nur anhand komplizierter und kostspieliger Prüf- und Messverfahren (zB Strom- und Signalmessungen im Nano- und Picoampere- bzw. -voltbereich; chemische und optische Technologien sowie kombinierte mechanische und elektronische Verfahren zur Analyse des Verhaltens integrierter Bausteine mit Probenadeln im Micrometerbereich) ermittelt werden können. Da die Anschaffungskosten für derartige Spezialprüf- und -messgeräte, die in der Regel nur im Herstellungsprozess verwendet werden können, außerordentlich hoch sind, sollen bestehende Infrastrukturen vor allem bei Herstellern von hochintegrierten elektronischen Bausteinen und anderen Technologieunternehmen genützt werden. Aus diesem Grund wird in § 7 Abs. 3 vorgesehen, dass die Bestätigungsstelle von sonstigen Unternehmen oder Einrichtungen sicherheitstechnische Prüfberichte zu Signaturprodukten und Verfahren einholen kann. Ein Vertrauensdiensteanbieter hat die Möglichkeit, seine Produkte und Verfahren der Bestätigungsstelle vorzulegen, die erforderlichenfalls ihrerseits Prüfberichte einholt. Er kann sich die nötigen Prüfberichte aber auch selbst beschaffen und diese der benannten Stelle zur Evaluierung vorlegen.

Im Rahmen ihrer Befugnisse obliegt die Beurteilung der anstehenden Fragen allein der Bestätigungsstelle. Bei ihren Stellungnahmen handelt es sich um gutachterliche Äußerungen gegenüber dem Antragsteller. Beschwerden über die Tätigkeit der benannten Stelle können an die Aufsichtsstelle herangetragen werden (Abs. 4).

Die Notifizierung von qualifizierten Signaturerstellungseinheiten, die von der benannten Stelle zertifiziert worden sind, wird gemäß Abs. 5 von der Aufsichtsstelle durchgeführt.

Zu § 8:

Für die Ausstellung von qualifizierten Zertifikaten müssen bestimmte Bedingungen eingehalten werden. Nach den Bestimmungen der eIDAS-VO hat ein qualifizierter VDA die Identität und gegebenenfalls die spezifischen Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat ausgestellt wird, zu überprüfen. Das eindeutige Feststellen der Identität der Zertifikatswerberin oder des Zertifikatswerbers ist Voraussetzung dafür, dass auf den Ersteller einer elektronischen Signatur geschlossen werden kann. Die Identitätsfeststellung hat entweder anhand eines amtlichen Lichtbildausweises oder durch einen anderen gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis zu erfolgen, wenn die Person oder Vertreter einer juristischen Person persönlich anwesend sind. Die Gleichwertigkeit zu einem amtlichen Lichtbildausweises dieses anderen Nachweises ist von der Aufsichtsstelle zu beurteilen. Zu denken wäre hier beispielsweise an eine bereits früher, aber gesichert dokumentierte, stattgefundene Identifizierung anhand eines Lichtbildausweises z. B. bei der Eröffnung eines Bankkontos. Wurde einer bestimmten Person von einem qualifizierten VDA bereits ein qualifiziertes Zertifikat ausgestellt, so ist für die Ausstellung weiterer Zertifikate durch denselben VDA keine neuerliche Identitätsfeststellung erforderlich. Vertreter von juristischen Personen haben darüber hinaus noch einen Nachweis (z. B. Gesellschaftsvertrag oder Firmenbuchauszug) über das Bestehen der Vertretungsbefugnis vorzulegen.

Die Identitätsfeststellung kann auch ohne persönliche Anwesenheit durch sonstige Identifizierungsmethoden vorgenommen werden, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten. Diese in Art. 24 Abs. 1 lit. d eIDAS-VO vorgesehene – relativ offene – Möglichkeit soll vor allem auch dem dynamischen technischen Fortschritt und innovativen Möglichkeiten Rechnung tragen. Ob in einem solchen Fall eine „gleichwertige“ Sicherheit im Sinne dieser Anforderung vorliegt, ist von Konformitätsbewertungsstellen zu beurteilen, die auch zur Durchführung einer Konformitätsbewertung von qualifizierten VDA nach Art. 20 eIDAS-VO berechtigt sind. Die Konformitätsbewertungsstelle hat dabei eine Gesamtbetrachtung anzustellen, in die eine Risikobewertung und das beim jeweiligen Alternativszenario vorhandene Missbrauchspotential einfließt. Es ist bei der Verwendung solcher Identifizierungsmethoden insbesondere auf eine bereits bei persönlicher Anwesenheit des Zertifikatswerbers erfolgte Identitätsfeststellung wie im ersten Absatz dieser Bestimmung vorgesehen, zurückzugreifen. Diese Identitätsfeststellung durch Vorlage eines amtlichen Lichtbildausweises oder eines sonstigen gleichwertigen, dokumentierten oder zu dokumentierenden Nachweises hat von einer vertrauenswürdigen Stelle durchgeführt zu werden. Vertrauenswürdige Stelle kann entweder der qualifizierte VDA selbst, ein anderer qualifizierter VDA oder jede andere Stelle, die einen vergleichbar hohen Sorgfaltsmaßstab wie ein qualifizierter VDA einzuhalten vermag, sein. Der das qualifizierte Zertifikat ausstellende qualifizierte VDA hat jedenfalls bei der Beurteilung der Vertrauenswürdigkeit jener Stelle, die die Identitätsfeststellung vorgenommen hat, jene notwendige Sorgfalt walten zu lassen, die auch notwendig wäre, wenn er die Identitätsfeststellung selbst vornehmen würde.

Zu § 9:

Diese Bestimmung betrifft den Fall, dass ein qualifizierter VDA seinen Betrieb (zur Gänze) einstellt und soll nach Möglichkeit sicherstellen, dass die Anwender-Signaturen auch nach Einstellung der Tätigkeit zuverlässig überprüft werden können. Die Verpflichtung des Abs. 1 trifft alle qualifizierten VDA gleichermaßen, während Abs. 2 lediglich jene qualifizierte VDA betrifft, die auch qualifizierte Zertifikate ausstellen.

Die Überprüfbarkeit der Anwender-Signaturen nach Einstellung der Tätigkeit des VDA setzt voraus, dass zumindest seine Zertifikatsdatenbank (Art. 24 Abs. 2 lit. k eIDAS-VO) – allenfalls auch die gesamte Dokumentation – von einem anderen qualifizierten VDA fortgeführt wird. Im Fall der Übernahme der Zertifikate (samt der Dokumentation nach Art. 24 Abs. 2 lit. h eIDAS-VO) durch einen anderen qualifizierten VDA liegt eine Vertragsübernahme vor, die jedoch ex lege nicht an die Zustimmung des Signators geknüpft ist, zumal dieser den Widerruf seines Zertifikats jederzeit veranlassen kann.

Findet eine Übernahme der Zertifikatsdatenbank nicht statt, so muss der qualifizierte VDA alle gültigen Anwender-Zertifikate widerrufen (Art. 24 Abs. 3 eIDAS-VO), sofern deren Weiterführung nicht im öffentlichen Interesse liegt (Abs. 3). Damit werden nähere Regelungen zum Beendigungsplan gem. Art. 24 Abs. 2 lit. i eIDAS-VO getroffen. Allfällige Ansprüche der Signatoren aus der vorzeitigen Beendigung des Vertragsverhältnisses bleiben unberührt. Im Interesse der Rechtssicherheit muss die Zertifikatsdatenbank jedoch jedenfalls weitergeführt werden, damit die vor der Einstellung der Tätigkeit ausgestellten qualifizierten Zertifikate ordnungsgemäß überprüft werden können (Art. 24 Abs. 4 eIDAS-VO). Nötigenfalls hat die Aufsichtsstelle auf Kosten des qualifizierten VDA hiefür Sorge zu tragen. Dabei sind von der Aufsichtsstelle nicht spezielle Datenbanksysteme oder Softwareprodukte weiter zu führen, sondern lediglich die darin enthaltenen Informationen in einer Weise bereit zu stellen, dass eine Überprüfung möglich ist. Es soll dadurch vermieden werden, dass der Aufsichtsstelle etwaige Lizenzkosten für proprietäre Datenbanksysteme entstehen.

Der Widerruf der bereits in Verwendung befindlichen qualifizierten Zertifikate ist aber nur dann zulässig, wenn deren Weiterführung nicht im öffentlichen Interesse liegt. Ein öffentliches Interesse liegt insbesondere vor, wenn Bürgerinnen und Bürger vor Behörden Amtswege elektronisch abwickeln oder behördliche Dokumente nachweislich elektronisch zugestellt bekommen wollen und im Zuge des Verfahrens eine eindeutige Identifikation der Antragstellerin bzw. des Antragstellers gefordert ist (vgl. dazu die Bestimmungen zur Bürgerkarte im E-Government-Gesetz (E-GovG)). Auch ersetzt die qualifizierte elektronische Signatur grundsätzlich die handschriftliche Unterschrift, weshalb es ohne Verwendung von qualifizierten Zertifikaten in vielen Fällen nicht mehr möglich wäre, rechtswirksame Erklärungen elektronisch abzugeben. Auch in diesem Fall stellt die Rechtsicherheit ein öffentliches Interesse dar. Ein Entfall ohne Weiterführung der qualifizierten Zertifikate hätte zudem weitreichende Konsequenzen etwa auch für den Justizbereich: Für Notare entfiele die elektronische Beurkundungssignatur der Notare, die der Errichtung öffentlicher Urkunden dient, was etwa auch den Wegfall der Einstellmöglichkeit und des Abrufs von Urkunden in das bzw. aus dem elektronische/n Urkundenarchiv des österreichischen Notariats bedeuten würde (in „Cyberdoc“ werden zB 2.700 Urkunden täglich neu eingestellt, derzeit sind etwa 7,5 Millionen Urkunden enthalten). Auch für Rechtsanwälte würde die Berufssignatur (elektronische Anwaltssignatur) entfallen, was etwa die Einstellmöglichkeit und Abrufmöglichkeit von Urkunden in das bzw. aus dem elektronische/n Urkundenarchiv der Rechtsanwaltschaft „Archivium“ bedeuten würde (derzeit werden etwa 2.500 -3.000 Urkunden täglich neu eingestellt, insgesamt sind zur Zeit etwa 2,8 Millionen Urkunden enthalten).

Durch die Weiterführung der qualifizierten Zertifikate wären insbesondere – nach Einstellung des jeweiligen qualifizierten VDA – alle Bürgerkarten weiter nutzbar, die auf einem solchen Zertifikat beruhen.

Die Absätze 2 und 3 implizieren, dass der Aufsichtsstelle bzw. dem Bund bestimmte Aufgaben zuerkannt werden. Damit diese Aufgaben erfüllt werden können, kann es notwendig sein technisch-organisatorische Vorkehrungen zu treffen, die als solche Teil der Vertrauensinfrastruktur iS der eIDAS-VO betrachtet werden können.

Zu § 10:

Die Dokumentation nach Art. 24 Abs. 2 lit. h eIDAS-VO sowie die Zertifikatsdatenbank müssen auch für gerichtliche oder behördliche Verfahren zur Verfügung stehen (Abs. 1). Das Auskunftsersuchen muss im Einklang mit den jeweils anwendbaren Verfahrensvorschriften stehen. Die Beschlagnahme oder Ausfolgung von Originalkopien nach anderen Rechtsvorschriften (insbesondere StPO) bleiben unberührt. Ein VDA hat in einem solchen Fall Duplikate anzufertigen, um seinen Pflichten weiterhin nachkommen zu können.

Ein VDA kann auch Zertifikate unter Verwendung eines Pseudonyms anstatt des Namens des Signators anbieten (vgl. Art. 3 Z 14 und Art. 28 Abs. 1 iVm Anhang I eIDAS-VO). Bei qualifizierten Zertifikaten müssen Pseudonyme kenntlich gemacht werden. Verhält sich ein unter einem Pseudonym handelnder Vertragspartner nicht vertrags- oder gesetzeskonform, so muss die Aufdeckung des Pseudonyms möglich sein. Die Voraussetzungen der Aufdeckung des Pseudonyms und damit der Preisgabe der wahren Identität des Signators, etwa zur Wahrung gesetzlicher Aufgaben (zB Aufklärung und Verfolgung von Straftaten) oder zur Durchsetzung von Rechtsansprüchen, richten sich gemäß § 10 Abs. 2 nach den einschlägigen Bestimmungen des Datenschutzgesetzes (§ 8 Abs. 1 Z 4 und Abs. 3 DSG 2000). Dies gilt insbesondere auch für das Auskunftsrecht (§ 26 DSG 2000) oder das Recht auf Richtigstellung oder Löschung (§ 27 DSG 2000) von Daten.

Bei der Verfolgung strafbarer Handlungen hat die Aufdeckung des Pseudonyms gegenüber den Strafverfolgungsbehörden zu erfolgen. In zivilrechtlichen Angelegenheiten muss die Aufdeckung – bei Vorliegen der gesetzlichen Voraussetzungen (§ 8 Abs. 1 Z 4 DSG 2000: überwiegende berechtigte Interessen eines Dritten) – gegenüber dem potentiellen Kläger erfolgen, weil eine Klagseinbringung unter Angabe eines Pseudonyms nicht möglich ist.

Aus Gründen der Rechtssicherheit wird in Abs. 3 generell die Aufbewahrungsdauer der Dokumentation mit 30 Jahren festgesetzt, was auch im Lichte der Vorgaben der eIDAS-VO als ein „angemessener Zeitraum“ angesehen werden kann. Zur Aufbewahrungsdauer der Zertifikatsdatenbank lässt die eIDAS-VO keinen Spielraum für nationale Regelungen. Als im Rahmen seiner Tätigkeit ausgegebene und empfangene Daten sind beispielsweise bei Diensten für Zustellung elektronischer Einschreiben ein empfangenes Zustellstück bzw. die Ausgabe eines Zeitstempels bei Zeitstempeldiensten gemeint.

Zu § 11:

Um den zwingenden Charakter der Verordnung auch im österreichischen Schadenersatzrecht abzubilden, wird in Abs. 1 angeordnet, dass die auch gegenüber dritten Personen bestehende Haftung von Vertrauensdiensteanbietern nach Artikel 13 Abs. 1 der eIDAS-VO – abgesehen vom Fall der in Artikel 13 Abs. 2 der eIDAS-VO geregelten Haftungsbegrenzung bei für dritte Beteiligte ersichtliche Beschränkungen der Verwendung der Dienste – im Vorhinein weder ausgeschlossen noch beschränkt werden kann.

Nach Artikel 13 Abs. 3 der eIDAS-VO werden die die Haftung regelnden Absätze 1 und 2 im Einklang mit den nationalen Vorschriften über die Haftung angewendet. In diesem Sinne wird in Abs. 2 konkretisierend ausgeführt, dass sich Umfang und Ausmaß des nach Artikel 13 der eIDAS-VO zu ersetzenden Schadens sowie allfällige Rückgriffsrechte gegenüber anderen Personen nach den auf den Schadensfall sonst anwendbaren Bestimmungen richten. Dazu zählen die Bestimmungen des Kollisionsrechts und des danach maßgeblichen österreichischen oder eines anderen zur Anwendung berufenen Sachrechts. Nach diesen Vorschriften richten sich daher insbesondere auch die Definitionen der in diesem Zusammenhang bedeutsamen Begriffe wie Schaden, Vorsatz und Fahrlässigkeit.

Nach Abs. 3 bleiben Ersatzansprüche gegenüber anderen Personen oder aus einem anderen Rechtsgrund unberührt. Damit wird klargestellt, dass die Haftungsbestimmung des Artikels 13 der eIDAS-VO der Inanspruchnahme anderer Personen oder von Vertrauensdiensteanbietern wegen anderer Sachverhalte als der Verletzung der in der eIDAS-VO festgelegten Pflichten nicht entgegensteht.

Zu § 12:

Nach Art. 17 Abs. 1 eIDAS-VO haben die Mitgliedstaaten eine Aufsichtsstelle zu benennen, die für die Wahrnehmung der Aufsichtsaufgaben verantwortlich ist. In Österreich kommt diese Funktion, wie auch schon bisher nach dem SigG, BGBl I. Nr. 190/1999 zuletzt geändert durch BGBl. I Nr. 75/2010, der Telekom-Control-Kommission zu. Es handelt sich dabei um eine nach § 116 TKG 2003 eingerichtete Behörde nach Art. 20 Abs. 2 B-VG.

Zur Erfüllung ihrer Aufgaben ist eine angemessene Ausstattung mit Ressourcen notwendig. Die Finanzierung der Tätigkeit der Aufsichtsstelle erfolgt dadurch, dass für die konkret erbrachten Leistungen von den VDA ein kostendeckendes Entgelt erbracht werden muss (§ 12 Abs. 2). Bedient sich die Aufsichtsstelle oder die RTR GmbH einer Bestätigungsstelle oder anderer benannten Stelle (§ 12 Abs. 3), so gehören die für die Tätigkeit der Bestätigungsstelle oder benannten Stelle auflaufenden Kosten zu den Kosten des Aufsichtsverfahrens, die ebenfalls von der Aufsichtsstelle vorzuschreiben sind.

Da die technische Sachkunde insbesondere bei der (oder den) Bestätigungsstellen nach § 7 konzentriert ist, kann die Aufsichtsstelle daher ein Gutachten einer Bestätigungsstelle einholen (§ 12 Abs. 3). Soweit dies aus technischer Sicht für die Durchführung der Aufsicht angezeigt erscheint, hat sich die Aufsichtsstelle mit einer Bestätigungsstelle oder einer anderen in einem Mitgliedstaat der EU gemäß Art. 30 Abs. 1 eIDAS-VO benannten Stelle abzustimmen.

In Abs. 4 wird die Weisungsfreiheit der Mitglieder der Aufsichtsstelle (wie in § 116 Abs. 3 TKG 2003) statuiert.

Zu § 13:

Zur Durchführung der operativen Aufsichtstätigkeit muss sich die Telekom-Control-Kommission der nach § 16 KOG eingerichteten, nicht gewinnorientierten Rundfunk und Telekom Regulierungs GmbH (RTR-GmbH) bedienen können (Abs. 1). Die RTR GmbH übt insbesondere vorbereitende und unterstützende Tätigkeiten für die Aufsichtsstelle aus.

In § 13 Abs. 2 wird ausdrücklich angeordnet, dass die RTR GmbH die Aufsichtsstelle in organisatorischer Hinsicht sowie im operativen Bereich zu unterstützen hat.

Zu § 14:

Die Aufgaben der Aufsichtsstelle ergeben sich unmittelbar aus den Regelungen der eIDAS-VO, insb. gemäß Art. 17. An einigen Stellen wird es jedoch den Mitgliedstaaten überlassen, darüber hinausgehende sonstige Aufgaben in nationalen Vorschriften vorzusehen.

Nach Art. 22 eIDAS-VO hat jeder Mitgliedstaat für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten VDA, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten enthalten, zu sorgen. Dabei ist der Durchführungsbeschluss (EU) 2015/1505, ABl. Nr. L 235/26 vom 9.9.2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten zu beachten.

Diese Aufgabe soll in Österreich von der RTR-GmbH übernommen und in einer für eine automatisierte Verarbeitung geeignete Form bereitgestellt werden. Nichtqualifizierte VDA können einen Antrag auf Aufnahme in die Vertrauensliste bei der Aufsichtsstelle stellen. In diesem Zusammenhang ist zu beachten, dass ein qualifizierter VDA nur in Hinblick auf einen konkreten von ihm erbrachten qualifizierten Vertrauensdienst als qualifizierter VDA zu werten ist. Für Vertrauensdienste die nicht qualifiziert sind, gilt der VDA als nichtqualifizierter VDA und die Aufnahme in die Vertrauensliste ist in diesem Fall nur auf Antrag möglich. Damit wird von der Möglichkeit gem. Art. 2 des Durchführungsbeschlusses (EU) 2015/1505, ABl. Nr. L 235/26 vom 9.9.2015, eine solche Regelung vorzusehen, Gebrauch gemacht.

Einer der Vertrauensdienste im Sinne der eIDAS-VO ist der (qualifizierte) Validierungsdienst gemäß Art. 33 und 40 eIDAS-VO. Die Validierung ist der Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur oder eines elektronischen Siegels. Die RTR-GmbH soll, wie auch schon bisher, unter www.signaturpruefung.gv.at ein technisches Service anbieten, mit dem qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel validiert werden können. In Abs. 2 erster Satz wird ausdrücklich darauf hingewiesen, dass dieses technische Service im öffentlichen Interesse betrieben wird und zur kostenfreien Nutzung jedermann bereitgestellt wird. Die RTR-GmbH ist daher kein VDA iSd der eIDAS-VO, da ein Vertrauensdienst im Sinne des Dienstleistungsbegriffs des EUV bzw. AEUV „in der Regel gegen Entgelt“ erbracht wird (Art. 3 Z 16 eIDAS-VO). Unbeschadet dieser Bestimmung steht es jedermann frei, einen (kostenpflichtigen) qualifizierten Validierungsdienst als qualifizierten Vertrauensdienst zu betreiben.

Der Signaturprüfdienst der RTR-GmbH ist eine Webanwendung, mit der sich elektronische Signaturen auch ohne die Installation spezieller Software prüfen lassen. Dabei werden Signaturen in den international genormten Formaten PADES, XMLDSIG und CMS ebenso unterstützt wie die in österreichischen E-Government-Anwendungen eingesetzten Formate (z. B. PDF-AS). Soweit Vertrauenslisten verfügbar und technisch ansprechbar sind, sind diese bei der Signaturprüfung auch heranzuziehen. Der Signaturprüfdienst basiert auf einem breit in Anwendung befindlichen Open Source Code, welcher am Stand der Technik gehalten wird. Von der Möglichkeit des Art. 17 Abs. 5 eIDAS-VO, eine Vertrauensinfrastruktur (§ 9) einzurichten, zu unterhalten und laufend zu aktualisieren, soll Gebrauch gemacht werden.

Zu § 15:

In § 15 Abs. 1 werden der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen (insbesondere den Bediensteten der RTR GmbH) die zur Vornahme der Aufsicht notwendigen prozessualen Eingriffsbefugnisse (Betretungs-, Besichtigungs- und Auskunftsrechte) eingeräumt. Der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen sind alle aufsichtsrelevanten Informationen zu erteilen und jede sonst erforderliche Unterstützung zu gewähren. Dies schließt jedenfalls auch die Einsicht in die betriebenen technischen Einrichtungen mit ein. Nach den jeweils anwendbaren Verfahrensvorschriften bestehende berufliche Verschwiegenheitspflichten und Aussageverweigerungsrechte bleiben unberührt.

Die Hilfeleistungspflicht der Organe des öffentlichen Sicherheitsdienstes nach § 15 Abs. 2 soll sicherstellen, dass die Aufsichtsmaßnahmen auch tatsächlich durchgeführt werden können.

§ 15 Abs. 3 sieht für die Vornahme der Aufsichtsmaßnahmen eine "Schonungsklausel" zugunsten der Betroffenen vor. Die eingesetzten Aufsichtsmittel müssen verhältnismäßig sein und sollen nicht die Sicherheit der Vertrauensdienste beeinträchtigen. Aufsichtsmaßnahmen dürfen also etwa nicht dazu führen, dass der private Signaturschlüssel des Vertrauensdiensteanbieters bekannt wird.

Zu § 16:

§ 16 normiert Verwaltungsstrafen einerseits für die missbräuchliche Verwendung fremder Signatur- und Siegelerstellungseinheiten (Abs. 1) sowie andererseits für Pflichtverletzungen von VDA (Abs. 3 bis 4).

In Abs. 3 soll eine Verwaltungsstrafe für die Unterlassung der Meldepflicht gem. Art. 19 Abs. 2 eIDAS-VO eingeführt werden. Art. 19 Abs. 2 eIDAS-VO kennt jedoch auch „andere einschlägige Stellen" denen zu melden ist. In Österreich wäre jedenfalls auch der Datenschutzbehörde zu melden. Bei Verstößen gegen das DSG 2000 ergeben sich dann auch allfällige andere Verwaltungsstrafen.

Werden verschiedene strafbare Handlungen durch eine Tat verwirklicht, dann sind diese mit dem Doppelbestrafungsverbot gem. Art 4 7. ZPMRK – EGMR nur dann vereinbar, wenn die strafbaren Handlungen nicht dieselben wesentlichen Elemente aufweisen (EGMR, Franz Fischer, 29.5.2001, 37.950/97). Dementsprechend liegt eine Verwaltungsübertretung gem. Abs. 1 bis 4 nur dann vor, wenn die Tat nicht auch nach anderen Verwaltungsstrafbestimmungen mit einer strengeren Strafe bedroht ist.

Zu § 17:

Diese Bestimmung enthält eine ausdrückliche Ermächtigung zur Erlassung einer Signatur- und Vertrauensdiensteverordnung. Sie bezieht sich insbesondere auf die Festlegung der Gebühren für die Aufsichtstätigkeiten und die Festsetzung näherer Anforderungen an qualifizierte Zertifikate und die Zertifikatsdatenbank.

Zu § 18 und 20:

Dabei handelt es sich um Bestimmungen zum Inkrafttreten und zum Vollzug des Gesetzes. Da die RL 1999/93 EG gemäß Art. 50 Abs. 1 eIDAS-VO aufgehoben wird, ist auch das SigG als österreichische Umsetzung dieser RL aufzuheben.

Zu § 19:

Art. 51 Abs. 2 eIDAS-VO ordnet die Übergangsregelung für qualifizierte Zertifikate in Abs. 1 bereits an, stellt jedoch auf qualifizierte Zertifikate, die gemäß der RL 1999/93 EG für natürliche Personen ausgestellt worden sind, ab. Diese RL wurde in Österreich durch das SigG umgesetzt. Diese Bestimmung stellt klar, dass Art 51 Abs. 2 auf qualifizierte Zertifikate, die aufgrund des SigG ausgestellt worden sind, anzuwenden ist.

In Abs. 2 wird eine Regelung getroffen, die der Rechtssicherheit bei der Verwendung bestehender nichtqualifizierter Zertifikate dient, insbesondere bei der in der Praxis weit verbreiteten Amtssignatur. Diese sollen weiterhin verwendet werden können. Nachdem Amtssignaturen im Regelfall fortgeschrittene Signaturen einer juristischen Person sind, soll mit dieser Bestimmung klargestellt werden, dass solche nichtqualifizierte Zertifikate nunmehr nach den Vorschriften der eIDAS-VO als nichtqualifizierte Zertifikate für fortgeschrittene elektronische Siegel weiter verwendet werden können.

Zu Artikel 2 (Änderung des E-Government-Gesetzes)

Zu Z 1 bis 6 (Inhaltsverzeichnis)

Es werden redaktionelle Anpassungen im Inhaltsverzeichnis vorgenommen.

Zu Z 7, 8, 9, 10, 11, 16 und 20 (Abschnittsüberschrift des 2. Abschnitts, § 2 Z 1, 4, 6, 10 und 11, § 2a, § 8 und § 14 Abs. 1)

Die eIDAS-VO enthält in ihrem Artikel 3 eine Vielzahl an Begriffsbestimmungen für den Bereich der elektronischen Identifizierung, die aufgrund des Rechtscharakters der EU-VO unmittelbar anwendbar sind. Die österreichischen Begriffsbestimmungen sind daher an die Definitionen der eIDAS-VO anzugleichen oder wo dies notwendig ist aufzuheben.

Die beispielhafte Aufzählung der Merkmale in Z 1 lehnt sich nun an die Personenidentifizierungsdaten im Sinne des Mindestdatensatzes des Anhangs der Durchführungsverordnung (EU) Nr. 1501/2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, ABl. Nr. L 235 vom 9.9.2015, an.

Zu Z 12 (§ 4 Abs. 2)

Nach den Vorgaben der eIDAS-VO können nur noch natürliche Personen Daten elektronisch signieren. Für nicht-natürliche Personen ist die Verwendung eines elektronischen Siegels vorgesehen, das den Ursprung und die Unversehrtheit der Daten sicherstellt mit denen das elektronische Siegel verbunden ist (Art. 3 Z 25 eIDAS-VO). Es soll daher überall dort, wo nach der bisherigen Rechtslage die Signatur der Stammzahlenregisterbehörde oder einer anderen Behörde vorgesehen war, nunmehr (auch) die Verwendung eines elektronischen Siegels möglich sein.

Zu Z 13 (§ 6 Abs. 4)

In § 6 Abs. 4 werden sprachliche und inhaltliche Redundanzen beseitigt.

Zu Z 14 (§ 6 Abs. 6)

Es soll sprachlich klargestellt werden, dass sich bei der Bildung der Stammzahl von natürlichen Personen die starke Verschlüsselung auf die ZMR-Zahl bzw. die Ordnungsnummer des Ergänzungsregisters bezieht.

Zu Z 15 (§ 7 Abs. 1)

Die Aufgaben der Stammzahlenregisterbehörde werden wie bisher durch die Datenschutzbehörde wahrgenommen. Mit der Streichung der ausdrücklichen Bezugnahme auf das Datenverarbeitungsregister wird lediglich der aktuellen organisatorischen Struktur der Datenschutzbehörde Rechnung getragen.

Zu Z 17 (Paragrafenüberschrift vor § 9)

Aus Gründen der besseren Verständlichkeit soll die Paragrafenüberschrift nicht nur wie bisher die Abkürzung „bPK“, sondern nun wieder auch den gesamten Begriff „bereichsspezifisches Personenkennzeichen“ umfassen.

Zu Z 18 (§ 10 Abs. 2)

Die Stammzahlenregisterbehörde soll ausdrücklich dazu berufen werden, vor allem bei einem sogenannten „Ausstattungsfall“, auch die Stammzahl nicht-natürlicher Personen zur Verfügung zu stellen. Dies erfolgt durch Abfrage beim Unternehmensregister. Die Abfrage des Unternehmensregisters durch die Stammzahlenregisterbehörde stellt einen zulässigen Anwendungsfall des § 25 Bundesstatistikgesetz dar.

Zu Z 19 (Überschrift 3. Abschnitt)

Da ausländische Services (§ 14a) nun ausdrücklich wie Datenanwendungen des privaten Bereichs behandelt werden, soll die Abschnittüberschritt dahingehend angepasst werden.

Zu Z 21 (§ 14a)

Ausländische Services sollen wie Datenanwendung des privaten Bereichs behandelt werden, wobei anstelle der Bereichskennung ein staatenspezifisches Kennzeichen oder bei Anwendungen internationaler Organisationen ein organisationsspezifisches Kennzeichen verwendet werden soll.

Zu Z 22 (§ 16 Abs. 2)

Neben einer elektronisch signierten Auskunft sollen nunmehr im Einklang mit Art. 35 eIDAS-VO auch elektronisch besiegelte Auskünfte möglich sein, da Registerauszüge in der Regel von der zuständigen Behörde als nicht-natürliche Person bestätigt werden. Vgl. auch die Erläuterungen zu Z 7.

Zu Z 23 (§ 17 Abs. 2)

Ein wesentliches Ziel von E-Government ist es, den Bürgerinnen und Bürgern ein verbessertes Service anbieten zu können. Auf Bürgerseite wird die Vorlage von Dokumenten (z. B. Meldezettel, Staatsbürgerschaftsnachweis, Geburtsurkunde), die der Behörde ohnehin bekannt sind oder zulässigerweise bekannt sein könnten, in der Praxis oftmals als lästig empfunden. Um die Vorlage von Nachweisen über bekannte Umstände zu reduzieren, soll die Neufassung des § 17 Abs. 2 nunmehr – bei Vorliegen der Voraussetzungen – eine umfassende Verpflichtung zur Abfrage sämtlicher elektronischer Register von Auftraggebern des öffentlichen Bereichs normieren und nicht mehr nur auf öffentliche Register abstellen. Weiters soll es nicht mehr darauf ankommen, dass die Datenprüfung in einem Verfahren als Vorfrage zu beurteilen ist. Dies hat bei der Anwendung der Bestimmung bei Behörden zu Auslegungsschwierigkeiten geführt und wurde oft zum Nachteil der Verwaltungskunden zu restriktiv ausgelegt.

Weder die geltende noch die vorgeschlagene Abfrageverpflichtung erweitert jedoch bestehende Ermittlungsbefugnisse von Behörden, weil ausschließlich auf eine bestehende Ermächtigung (gesetzlich oder gewillkürt) zurückgegriffen werden muss. Weiterhin obliegt es der Organisationsgewalt der

jeweiligen Behörde, die technischen Zugänge zu den Registern zu schaffen. Die konsequenten Registerabfragen erhöhen die Datenqualität bei Behörden, weil etwa Fehlerquellen durch Abtippen entfallen. Mittelfristig führt der geringere Manipulationsaufwand bei der Datenpflege zu Entlastungen der Behörden und zur Steigerung der Datenqualität.

Schließlich wird mit der geplanten Ergänzung des § 17 Abs. 2 einem EU-weiten Trend Rechnung getragen: Die Europäische Kommission unterstreicht in ihrer rezenten Mitteilung über eine „Strategie für einen digitalen Binnenmarkt für Europa“ (COM (2015) 192 final vom 6.5.2015) die entscheidende Rolle von E-Government Diensten, wenn es darum geht, die Kosteneffizienz und Qualität der für Bürger und Unternehmen erbrachten Dienstleistungen zu erhöhen und hebt als ein Beispiel für eine Effizienzsteigerung den „Grundsatz der einmaligen Erfassung („Once only“)“ hervor. So würden öffentliche Verwaltungen in nur 48 % der Fälle Angaben über die Bürger oder Unternehmen weiter verwenden, die ohnehin bereits im Besitz der Verwaltungen sind. In der Mehrzahl der Fälle würde es hingegen zu erneuten Abfragen kommen. Nach Auffassung der Kommission könnten durch eine konsequente Anwendung dieses Grundsatzes beträchtliche Einsparungen erzielt werden, wobei freilich strikt auf die Einhaltung der Datenschutzvorschriften zu achten ist.

Zu Z 24 (§ 17 Abs. 3 Z 2)

Neben einer elektronisch signierten Meldebestätigung sollen nunmehr im Einklang mit Art. 35 eIDAS-VO auch elektronisch besiegelte Meldebestätigungen möglich sein, da Registerauszüge in der Regel von der zuständigen Behörde als nicht-natürliche Person bestätigt werden. Vgl. auch die Erläuterungen zu Z 7.

Zu Z 25 und 26 (§ 19 Abs. 1 und 3)

Durch die Aufhebung des Signaturgesetzes aufgrund der unmittelbar anwendbaren eIDAS-VO müssen die technischen Anforderungen an die Amtssignatur angepasst werden. Dabei soll nunmehr anstelle der Mindestanforderung der fortgeschrittenen elektronischen Signatur auch ein fortgeschrittenes elektronisches Siegel gemäß Art. 36 eIDAS-VO möglich sein. Das technische Sicherheitsniveau bleibt damit unverändert und die technischen Anforderungen für Auftraggeber des öffentlichen Bereichs ebenso.

Da nunmehr auch elektronische Siegel zur Erstellung der Amtssignatur möglich sein sollen, sind in Abs. 3 vom Auftraggeber des öffentlichen Bereichs auch die entsprechenden Informationen zur Prüfung des elektronischen Siegels bereitzustellen.

Zu Z 26 bis 28, 30 und 31 (§ 22, § 24, § 25, § 26)

Es werden redaktionelle Anpassungen vorgenommen.

Zu Z 27 (§ 24 Abs. 4)

Die Änderungen im E-GovG zur Durchführung der eIDAS-VO sollen zeitgleich mit dem SVG am 1. Juli 2016 in Kraft treten.