# Vertrauensdienste oder Bärendienste? Rechtsicherheit von Kundenportalen, Blockchain & Co durch und neben der eIDAS-VO

*Paul C. Johannes*

## *I. Einleitung*

Die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)[1] ist am 17.9.2014 in Kraft getreten und ihre materiellen Regelungen gelten seit dem 1.7.2016. Dabei stellt sich die Frage, wie sich das deutsche Recht seitdem im Hinblick auf die nach der eIDAS-VO geregelten Vertrauensdienste entwickelt hat und welche Verzahnungen erfolgten. Der Beitrag stellt die eIDAS-VO vor (II.), erklärt deren Vorgaben für Vertrauensdienste (III.) und bringt dies in Verbindung zu deutschen Regelungen und anderen Diensten, die Vertrauen im elektronischen Rechts- und Geschäftsverkehr schaffen sollen (IV.), um so das Verhältnis zwischen EU-Verordnung und nationalem Recht zu bewerten und zu beantworten, ob es sich bei Vertrauensdiensten außerhalb der eIDAS-VO um Bärendienste handelt (V.).

## *II. eIDAS-VO und Vertrauensdienstegesetz (VDG)*

### *1. Inhalt und Zielsetzung der eIDAS-VO*

Elektronische Transaktionen in Wirtschaft und Verwaltung benötigen Sicherungsmittel wie Signaturen und Zeitstempel, um Manipulationen zu verhindern, bestimmte Formen für Willenserklärungen einzuhalten und Beweissicherheit zu gewährleisten. Um diese zusammenhängend zu regeln, hat die Union am 23.7.2014 die eIDAS-VO erlassen.[2] Deren Ziel ist es

1 ABl. EU L 257/73.

2 Zu Entstehungsgeschichte und Entwurf *Roßnagel/Johannes*, Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – Neue Regeln für elektronische Sicherheitsdienste, ZD 2013, 65.

unter anderem, einen einheitlichen europäischen Markt für elektronische Sicherungsmittel zu schaffen und hierdurch das Vertrauen in den elektronischen Rechtsverkehr in der EU zu stärken. Die eIDAS-VO sieht zu diesem Zweck Vorgaben zur Vereinfachung und Harmonisierung der Nutzung von elektronischen Signaturen und vergleichbaren Identifikationssystemen vor, die für alle EU-Mitgliedstaaten unmittelbar und verbindlich gelten.

Neben allgemeinen Bestimmungen enthält die eIDAS-VO vor allem zwei voneinander getrennte inhaltliche Regelungskomplexe: einen zur Koordination nationaler Systeme zur elektronischen Identifizierung[3] und einen zur unionseinheitlichen Regelung von Vertrauensdiensten.[4] Im Folgenden werden nur die Regelungen zu Vertrauensdiensten betrachtet.[5]

### 2. *Anwendungsbereich*

Die eIDAS-VO gilt nach Art. 1 Abs. 1 i.V.m. Art. 4 für unionsweit angebotene Vertrauensdienste. Sie gilt gem. Art. 288 AEUV ohne nationalen Umsetzungsakt unmittelbar in jedem Mitgliedstaat und ist für Unionsbürger und staatliche Stellen verbindlich.[6] Sie hat Anwendungsvorrang gegenüber nationalen Regelungen. Zur Anwendbarkeit genügt die grundsätzliche Möglichkeit, dass die Vertrauensdienste grenzüberschreitend zum Einsatz kommen. Die eIDAS-VO gilt damit für alle in der Union niedergelassenen Anbieter von Vertrauensdiensten. Nach Erwägungsgrund 24 will sie erreichen, dass „Vertrauensdienste, die dieser Verordnung entsprechen, [...] im Binnenmarkt frei verkehren können".

Gem. Art. 2 Abs. 2 eIDAS-VO findet die Verordnung keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet wer-

3 Dazu *Spindler/Rockenbauch*, Die elektronische Identifizierung – Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, MMR 2013, 139.

4 Die Anhänge I, III und IV enthalten jeweils kurze Anforderungslisten für qualifizierte Zertifikate für elektronische Signaturen, elektronische Siegel und Website-Authentifizierung und Anhang II enthält Anforderungen an „qualifizierte Signaturerstellungseinheiten".

5 Zur eID und Entwicklung im deutschen Recht vgl. *Beck*, Elektronische Identifizierung leicht(er) gemacht, DÖV 2018, 1042.

6 EuGH, Rs. C-43/71, ECLI:EU:C:1971:122, Rn. 9 – Politi.

den. Auch rein innerstaatliche Sachverhalte können damit ausschließlich durch nationale Vorschriften geregelt werden, sogar wenn diese im Widerspruch zur eIDAS-VO stehen.[7]

Außerdem findet die Verordnung gem. Art. 2 Abs. 3 eIDAS-VO keine Geltung in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder auf andere rechtliche oder verfahrensmäßige Formvorschriften.

Nationale Vorschriften behalten gegenüber der eIDAS-VO grundsätzlich ihre Gültigkeit und können sogar die Regelungen der eIDAS-VO ergänzen und konkretisieren, soweit sie inhaltlich nicht im Widerspruch zu diesen stehen.[8] Der Gesetzgeber darf kein gegen Unionsrecht verstoßendes Recht setzen.[9]

### *3. Vertrauensdienstegesetz (VDG)*

Die eIDAS-VO gilt in den Mitgliedstaaten unmittelbar, d. h. sie bedarf hinsichtlich ihrer materiellen Vorschriften grundsätzlich keiner Umsetzung in nationales Recht. Geschaffen werden müssen jedoch die erforderlichen Voraussetzungen für den effektiven Vollzug der Verordnung. Dies betrifft u. a. Öffnungsklauseln, Regelungen zu Zuständigkeiten und Befugnissen der beteiligten Behörden und nationale Regelungen zur Präzisierung.[10] Die eIDAS-VO hat die Signaturrichtlinie[11] aufgehoben. Jene war in Deutschland durch das Signaturgesetz (SigG) und die Signaturverordnung (SigV) umgesetzt. Diese sowie die Regelungen zur Anwendung der elektronischen Signaturen in weiteren nationalen Gesetzen wie dem VwVfG oder der ZPO galten auch mit Anwendbarkeit der eIDAS-VO weiter. Am 29.7.2017 trat jedoch das Vertrauensdienstegesetz (VDG) als Art. 1 des eIDAS-Durchführungsgesetzes[12] in Kraft. Es ersetzte das SigG und die SigV. Weitere Artikel des eIDAS-Durchführungsgesetzes passten das deut-

---

7 *Roßnagel*, Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?, MMR 2015, 359, 360.

8 *Roßnagel*, MMR 2015 (Fn. 7), 360.

9 EuGH, Rs. C-74/86, ECLI:EU:C:1988:198, Rn. 10 – Kommission/Deutschland; EuGH, Rs. C-106/77, ECLI:EU:C:1978:49, Rn. 17, 18 – Simmenthal II.

10 Zum Regelungsbedarf und -spielraum ausführlich *Roßnagel*, Das Recht der Vertrauensdienste – Die eIDAS-Verordnung in der deutschen Rechtsordnung, Baden-Baden 2016, 77 ff.

11 RL 1999/93/EG, EG ABl. L 13 v. 19.1.2000, S. 12.

12 Dazu *Johannes*, Entwurf des eIDAS-Durchführungsgesetzes in der Ressortabstimmung, ZD-Aktuell 2016, 05423.

sche Recht für Vertrauensdienste an die eIDAS-Verordnung an. Die wesentlichen Regelungen zu Vertrauensdiensten enthält die eIDAS-VO. Das VDG kann wegen des Anwendungsvorrangs der Verordnung nur präzisierende, konkretisierende und ergänzende Regelungen enthalten.[13] Das VDG wird seinerseits durch die Vertrauensdiensteverordnung (VDV) vom 15.2.2019 näher ausgestaltet.[14]

### *4. Aufsicht*

Mit § 2 VDG wurden der Regelungsauftrag des Art. 17 eIDAS-VO erfüllt, nationale Aufsichtsbehörden zu bestimmen. Aufsichtspflicht und -aufgaben[15] wurden aufgeteilt zwischen der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Die BNetzA ist Aufsichtsbehörde für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel und elektronische Einschreiben-Zustelldienste und das BSI für Webseiten-Zertifikate. Im Zusammenhang mit Vertrauensdiensten kommen dem BSI weitere Aufgaben zu, insbesondere die Erstellung technischer Standards, die Bewertung von Algorithmen und zugehörigen Parametern sowie die Erstellung technischer Vorgaben und die Bewertung technischer Standards für den Einsatz von Vertrauensdiensten in Digitalisierungsvorhaben nach Maßgabe der entsprechenden Fachgesetze.[16]

Die Aufsichtsbehörden können nach § 4 Abs. 1 VDG zur Durchsetzung der eIDAS-VO, des VDG und der VDV gegenüber Anbietern von Vertrauensdiensten die erforderlichen Maßnahmen treffen. Sie können von ihnen Nachweise anfordern und selbst Überprüfungen vornehmen und dazu die in Art. 17 Abs. 4 eIDAS-VO geregelten Aufsichtsbefugnisse nutzen.

## *III. Vertrauensdienste*

Die eIDAS-VO will die Vorschriften für elektronische Signaturen „stärken und erweitern" (EG 3) und auf weitere elektronische Sicherheitsdienste anwenden. Ein „Vertrauensdienst" ist nach Art. 3 Nr. 16 eIDAS-VO „ein elek-

13 *Roßnagel*, Das Vertrauensdienstegesetz, MMR 2018, 31.
14 BGBl. I S. 114.
15 Vgl. Art. 17 Abs. 3 und 4 eIDAS-VO.
16 *Roßnagel*, MMR 2018 (Fn. 13), 32.

tronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht:

a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder
b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder
c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten".

Vertrauensdienste können einfach,[17] fortgeschritten oder qualifiziert sein. Die jeweiligen Anforderungen ergeben sich aus der eIDAS-VO, wobei die Einstufung aufeinander aufbaut.[18]

### *1. Einfache Vertrauensdienste*

Für einfache „Vertrauensdienste" gelten nur wenige allgemeine und spezielle Vorschriften. Für sie enthält Art. 19 eIDAS-VO allgemeine Sicherheitsanforderungen. Dazu gehört die Verpflichtung, die Dienste durch „geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken" zu schützen, die den Stand der Technik berücksichtigen. Sicherheitsverletzungen müssen den zuständigen Aufsichtsstellen gemeldet werden. Auch einfache Vertrauensdienste unterliegen nach Art. 17 Abs. 3 lit. a eIDAS-VO der ex post Aufsicht der nationalen Aufsichtsstellen.

Die Anbieter haften nach Art. 13 eIDAS-VO für vorsätzlich oder fahrlässig zugefügte Schäden, die auf eine Nichterfüllung der Anforderungen der Verordnung zurückzuführen sind. Hierfür trägt der Geschädigte die Beweislast. Sie können diese Haftung einschränken, wenn sie Verwendungsbeschränkungen ihrer Dienste für Dritte ersichtlich machen.[19] Für einfache Vertrauensdienste und elektronische Dokumente (Art. 46 eIDAS-VO) bestimmt die eIDAS-VO, das diesen die Zulässigkeit als Beweismittel in

17 Die eIDAS-VO verwendet nicht die Wertung „einfach", er ist ein an allgemein anerkannter Sammelbegriff für die Definition der jeweiligen Vertrauensdienste.

18 Fortgeschrittene Vertrauensdienste erfüllen die Anforderungen an einfache; qualifizierte Vertrauensdienste sind fortgeschrittenen Vertrauensdienste, die zusätzlich die einschlägigen Anforderungen der eIDAS-VO erfüllen.

19 *Roßnagel*, Neue Regeln für sichere elektronische Transaktionen, NJW 2014, 3686, 3688.

Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil sie in elektronischer Form vorliegen. Dies korrespondiert im Ergebnis zu § 371 ZPO, wonach auch elektronische Dokumente als Objekte des Augenscheins zunächst der freien richterlichen Beweiswürdigung unterliegen.

### 2. *Qualifizierte Vertrauensdienste*

Ein „qualifizierter Vertrauensdienst" ist ein Vertrauensdienst, „der die einschlägigen Anforderungen dieser Verordnung erfüllt". Für ihn gelten zusätzlich zu den Anforderungen für einfache Vertrauensdienste vor allem die besonderen Anforderungen der Art. 20 bis 24 eIDAS-VO und die jeweils dienstspezifischen Anforderungen der Art. 25 bis 45 eIDAS-VO.[20] Sie bewirken weitergehende Rechtsfolgen als für einfache Vertrauensdienste, insbesondere höhere Beweiskraft.[21]

Eine elektronische Signatur gem. Art. 3 Nr. 10 eIDAS-VO sind Daten in elektronischer Form, die anderen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Verwender zum Unterzeichnen verwendet. Ein elektronisches Siegel ist eine elektronische Signatur einer juristischen Person. Ein elektronischer Zeitstempel bezeichnet nach Art. 3 Nr. 33 eIDAS-VO Daten in elektronischer Form, die andere elektronische Daten mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese Daten zu diesem Zeitpunkt vorhanden waren. Ein elektronisches Einschreiben dient dazu, die Übermittlung von Daten mit elektronischen Mitteln nachweisen zu können und die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung zu schützen. Zertifikate für die Website-Authentifizierung sollen Betrug im Internet erschweren.[22]

### 3. *Weitere Vertrauensdienste*

Nach Erwägungsgrund 25 eIDAS-VO steht es „den Mitgliedstaaten [...] frei [...], auch andere Arten von Vertrauensdiensten zusätzlich zu jenen festzu-

20 Ausführlich *Roßnagel*, NJW 2014 (Fn. 19), 3689.
21 Dazu ausführlich *Jandt*, Beweissicherheit im elektronischen Rechtsverkehr, NJW 2015, 1205; *Roßnagel*, Beweiswirkungen elektronischer Vertrauensdienste, MMR 2016, 647.
22 Ausführlich *Roßnagel*, NJW 2014 (Fn. 19), 3689 f.

legen, die auf der in dieser Verordnung vorgesehenen abschließenden Liste der Vertrauensdienste stehen, um diese auf nationaler Ebene als qualifizierte Vertrauensdienste anzuerkennen".[23]

## *IV. Vertrauensdienste außerhalb der eIDAS-VO?*

Nicht alle Arten von Diensten und Technologien, die derzeit im elektronischen Rechts- und Geschäftsverkehr verwendet werden, um Vertrauen zu stiften und für Sicherheit zu sorgen, lassen sich ohne weiteres unter die in der eIDAS-VO definierten Vertrauensdienste subsumieren. Sind solche Dienste aber gleich Bärendienste? Bärendienste in dem Sinne, als dass sie Sicherheit versprechen, möglicherweise aber nicht unter den Schirm der gesetzlichen Regulierung und Aufsicht fallen. Eventuell verwenden solche Dienste Vertrauensdienste der eIDAS-VO, unterliegen aber spezifischen nationalen Regeln. Gerade auch im Hinblick auf die Möglichkeit der Mitgliedstaaten, eigene qualifizierte Vertrauensdienste zu definieren, stellt sich für Deutschland die Frage nach der Verflechtung und Verzahnung deutscher Gesetze und der Rechts- und Anwendungspraxis des elektronischen Rechtsverkehrs mit den Vorgaben der eIDAS-Verordnung.

### *1. De-Mail und andere elektronische Postdienste*

Bekanntes Beispiel für einen deutschen Kommunikationsdienst, der für Vertrauen und Rechtssicherheit sorgen soll und der spezifischen deutschen Regeln unterliegt, ist die De-Mail.

„De-Mail-Dienste" sind Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen. Ein „De-Mail-Dienst" muss nach dem De-Mail-Gesetz (DeMailG) „eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post sowie die Nutzung eines Verzeichnisdienstes und kann zusätzlich auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglichen". Ein De-Mail-Dienst darf nur von einem akkreditierten Diensteanbieter betrieben werden.

Das DeMailG sieht vor, dass der DeMail-Anbieter Vertrauensdienste einsetzen kann und teilweise muss. Nach § 3 Abs. 2 Nr. 1 lit. d DeMailG kann

---

23 *Roßnagel*, MMR 2015 (Fn. 7), 362.

bei Kontoeröffnung die Identität eines Nutzers anhand einer qualifizierten elektronischen Signatur überprüft werden. Der in § 5 DeMailG geregelte Postfach- und Versanddienst wird u.a. dadurch realisiert, dass der Anbieter nach Abs. 4 S. 3 Nachrichten im Auftrag des Senders mit einer qualifizierten elektronischen Signatur versehen muss. Nach Abs. 7 S. 3, Abs. 8 S. 5 und Abs. 9 S. 6 müssen auch die Versand-, Empfangs- und Abholbestätigung mit einer qualifizierten elektronischen Signatur des DeMail-Anbieters versehen werden. Dies gilt auch für die Identitätsbestätigung nach § 6 Abs. 1 DeMailG und das Protokoll zur Dokumentenablage nach § 8 S. 5 DeMailG.

Hinsichtlich qualifizierter Dienste für die Zustellung elektronischer Einschreiben regelt § 18 VDG das Verhältnis zu den nach DeMailG akkreditierten Zustelldiensten. Beantragt ein akkreditierter De-Mail-Anbieter den Status eines qualifizierten Dienstes für die Bestätigung der Zustellung elektronischer Einschreiben, soll die Konformitätsbewertungsstelle die Konformitätsbewertung nach Möglichkeit auf die Prüfung der Nachweise beschränken, die im Rahmen der Akkreditierung nach § 18 Abs. 3 DeMailG erbracht worden sind. DeMail-Anbieter können also, müssen aber nicht zwingend, qualifizierte Vertrauensdienstleister sein. Wollen sie auch als qualifizierter Dienst für elektronische Einschreiben handeln können, unterliegen sie sowohl den Anforderungen der eIDAS-VO als auch denen des DeMailG.

### 2. *Das besondere elektronische Anwalts-, Notar- und Behördenpostfach*

Ein anderes Beispiel für einen deutschen Kommunikationsdienst ist das besondere Anwaltspostfach (beA). Das beA ist ein den Rechtsanwälten zur Verfügung stehendes Postfach zwecks Teilnahme am elektronischen Rechtsverkehr. Das beA löst das bisherige Gerichts- und Verwaltungspostfach (EGVP) ab. Das beA dient der elektronischen Kommunikation zwischen den Gerichten und der Anwaltschaft sowie zwischen den Rechtsanwälten untereinander. Alle Gerichte bundesweit nehmen am elektronischen Rechtsverkehr teil und sind über das beA erreichbar. Umgekehrt können die Gerichte und auch Behörden ihre Post über das beA an die Rechtsanwälte zustellen, die insoweit zumindest eine passive Nutzungspflicht zur Kenntnisnahme haben. Das beA hat die Funktionalität eines elektronischen Zustelldienstes. Es ist aber für eine geschlossene Benutzer-

gruppe eingerichtet und unterliegt daher nicht den Regelungen für Vertrauensdienste nach der eIDAS-VO.[24]

Das beA eröffnet einen sicheren Übermittlungsweg nach § 130a Abs. 4 Nr. 2 ZPO zur Übersendung von Schriftsätzen an Gerichte. Dies ersetzt die ansonsten erforderliche eigenhändige Unterschrift und erfordert auch keine qualifizierte Signatur der unterzeichnenden Person.[25] Unbenommen bleibt Rechtsanwälten die Kombination beider Möglichkeiten, nämlich (bestimmende) Schriftsätze über beA einzureichen und zusätzlich qualifiziert zu signieren. Grundlage für den elektronischen Rechtsverkehr und zur Realisierung des besonderen elektronischen Anwaltspostfachs (beA) ist das Gesetz zur Einführung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013 (ERV-Gesetz). Näheres zu Einrichtung und zum Betrieb des beA regelt § 31a BRAO und die Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (RAVPV).

Ein dem beA vergleichbarer Dienst wurde für Notare mit dem besonderen elektronischen Notarpostfach geschaffen. Die rechtliche Grundlage bildet § 78n BNotO. Näheres regelt die Verordnung über das Notarverzeichnis und die besonderen elektronischen Notarpostfächer (NotVPV).

### *3. Kunden-Postfächer und Portalkommunikation*

De-Mail und beA sind Beispiele für national besonders geregelte Vertrauensdienste und deren Verwendung. Daneben existieren im elektronischen Geschäftsverkehr eine Vielzahl von Diensten und Technologien, die zwar Vertrauen unter den Verwendern schaffen sollen, aber nicht besonders gesetzlich reguliert sind. Zum Beispiel gehen viele Unternehmen[26] dazu über, ihre Nachrichten, Abrechnungen und Kundenmitteilungen auf den unternehmenseigenen Portalen abzulegen, anstatt diese per Briefpost oder

---

24 *Roßnagel*, MMR 2015 (Fn. 7), 361.

25 Zum Problem der Fremdeinreichung und Containersignatur BAG, Beschl. v. 24.10.2019 – 8 AZN 589/19; *Müller*, Fehlende Personenidentität zwischen beA-Postfachinhaber, einfacher Signatur und qualifizierter Signatur, NZW 2019, 1682; *Ulrich/Schmieder*, Die elektronische Einreichung in der Praxis, NJW 2019, 113.

26 Z.B. Banken, Versicherungen, Kreditkarten- oder Telekommunikationsanbieter sowie Strom- und Gasversorger.

E-Mail zu versenden.[27] Das Kundennachrichtenkonto richtet das Unternehmen regelmäßig selbst für den Kunden ein. Dieser braucht nur die persönlichen Zugangsdaten (insbesondere das Passwort) zu generieren. So entsteht eine portalbasierte Mailbox als „Portalbox".[28] Der Wechsel von der E-Mail-Kommunikation zur Portalkommunikation wirft zahlreiche Rechtsfragen auf, insbesondere hinsichtlich des Zugangs von Nachrichten, der Einhaltung von Formvorschriften und der Beweiskraft der Dokumente.[29] Durch den Einsatz von Vertrauensdiensten nach der eIDAS-VO unter Einbindung von Vertrauensdiensteanbietern können Unternehmen Kommunikationsportale konzipieren, die sowohl den Unternehmensinteressen (rechtssicherer Zugang) als auch den Bedürfnissen der Kunden (zentrale Abrufbarkeit) Rechnung tragen.[30]

### *4. „Oder elektronisch" im Verwaltungsrecht*

Die Kunden-Postfächer und Portalkommunikation sind ein Zeichen dafür, dass Wirtschaft und Bürger nicht ohne Weiteres den Einführungsaufwand und die Kosten, die mit der Verwendung von qualifizierten Vertrauensdiensten einhergehen können, tragen wollen. Dies dürfe einer Abwägung der Kosten und Nutzen folgen. Eine vergleichbare Problematik hat der Gesetzgeber auch in Bezug auf die Verwendung von Vertrauensdiensten zum Ersatz der Schriftform festgestellt und reagiert.

Das „Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes vom 29.3.2017" änderte in 181 unterschiedlichen Gesetzen und Verordnungen 476 Rechtsvorschriften. Dabei strich es einige Schriftformerfordernisse ganz und ergänzte viele Vorschriften um die Möglichkeit der Nutzung einfacher elektronischer Verfahren.[31] Dadurch wurde im Verwaltungsrecht eine neue Formvorschrift sui generis geschaffen, welche unterhalb der Anforderungen der elektronischen Form

27 *Heckmann*, Rechtsfragen elektronischer Bereitstellung von Nachrichten und Dokumenten über ein Sammelportal-Postfach als Dienst nach der eIDAS-Verordnung, CR 2016, 684, 685.
28 *Heckmann*, CR 2016 (Fn. 27), 685.
29 *Lehmann/Rettig*, Rechtliche Vorgaben für Kunden-Online-Postfächer, NJW 2020, 569.
30 *Heckmann*, CR 2016 (Fn. 27), 693 ff.
31 Siehe dazu bereits *Johannes*, Bundestag: Gesetz zum Abbau der Schriftform im Verwaltungsrecht des Bundes beschlossen, ZD-Aktuell 2017, 05489.

liegt und den Einsatz von zum Beispiel einfachen E-Mails oder Nachrichten über Messengerdienste ermöglicht.

Das Gesetz ist im Kontext langjähriger Bemühungen zur Modernisierung der Verwaltungskommunikation zu sehen. Bereits in der „Digitalen Agenda 2014 – 2017" der Bundesregierung, die dem Regierungsprogramm „Digitale Verwaltung 2020"[32] zu Grunde liegt, wird die Überprüfung verwaltungsrechtlicher Formerfordernisse als eine Maßnahme genannt.[33] Dazu wurde ein breit angelegtes Normenscreening durchgeführt.[34] So wurden Schriftformerfordernisse identifiziert, die ersatzlos gestrichen werden oder die durch elektronische Verfahren ersetzt wurden.

Bei der überwiegenden Zahl der gestrichenen oder ergänzten Schriftformerfordernisse handelt es sich eher um Fälle mit begrenzter Relevanz für Bürger und Unternehmen. Es sind solche, die geschätzte Fallzahlen von weniger als 1.000 pro Jahr aufweisen.[35] So darf zum Beispiel die Erlaubnis zum Führen zusätzlicher Bezeichnungen zum Schutz gegen Wellenschlag, wie etwa einem roten Licht bei Nacht, an Fahrzeugen auf der Donau gemäß § 3.48 Nr. 2 lit. b der Anlage A zur Donauschifffahrtspolizeiverordnung durch die zuständige Behörde nun auch – „Endlich!" will man ausrufen – elektronisch erfolgen. Es wurden aber auch Schriftformerfordernisse in Regelungen gestrichen oder ergänzt, die bundesweit eine sehr hohe Zahl von Verfahren betreffen, wie z.B. bei Einwendungen im Planfeststellungsverfahren nach § 74 Abs. 5 S. 4 VwVfG und bei Entscheidungen im Sinne von § 14 Bundeskindergeldgesetz oder zum Unterhaltsvorschuss nach § 9 Abs. 2 Unterhaltsvorschussgesetz.

Zu beachten ist, dass mit dem Zusatz „oder elektronisch" in den geänderten Rechtsvorschriften nicht die elektronische Form gemeint ist, wie sie in § 126 a BGB definiert ist. Gemeint sind auch nicht Ersatzmöglichkeiten der Schriftform nach § 3 a Abs. 2 VwVfG, also die qualifizierte elektroni-

---

32 Bundesregierung, Digitale Verwaltung 2020, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/regierungsprogramm-digitale-verwaltung-2020.pdf?__blob=publicationFile&v=4, 2014.

33 Bundesregierung, Digitale Agenda 2014 – 2017, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3, 2014, 9.

34 Bericht der Bundesregierung zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes, BT-Drs. 18/9177.

35 Vgl. Stellungnahme des Nationalen Normenkontrollrates, NKR-Nr. 3703 vom 21. Juli 2016, 3, https://www.normenkontrollrat.bund.de/Webs/NKR/Content/DE/Download/2016-07-21_3703_download__bmi_abbau-schriftformerfordernis.pdf.

sche Signatur nach eIDAS, De-Mail mit Absenderbestätigung, das elektronische Formular mit nPA-Identifizierung oder ein anerkanntes Bürgerportal. Diese Möglichkeiten bestanden ohnehin schon.

„Elektronisch" soll zur Vereinfachung der Verwaltungskommunikation bedeuten, dass die Behörde grundsätzlich auch einfachere Kommunikationsmethoden, wie z.B. einfache E-Mail oder eine Messenger-Nachricht verwenden kann. Die Gesetzesbegründung stellt klar, dass der Einsatz solcher einfachen elektronischen Kommunikationsmethoden zum einen von der tatsächlichen Zugangseröffnung auf Seiten des Empfängers abhängig ist.[36] Zum anderen läge deren Einsatz im Ermessen der Behörden.[37] Es wird darauf hingewiesen, dass die jeweiligen Verwaltungen zu gewährleisten haben, dass auf personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei ihrer Speicherung nicht unbefugt zugegriffen werden kann. Dies könne insbesondere durch Verschlüsselungsverfahren sichergestellt werden, die dem Stand der Technik entsprechen. Der Einsatz bestimmter elektronischer Verfahren wird nicht näher festgelegt. Dies soll eine größtmögliche Verfahrensflexibilität erlauben, da die jeweilige Behörde nach ihrem Ermessen und ohne gesetzliche Verpflichtung zur Nutzung eines bestimmten elektronischen Verfahrens beurteilen könne, welche Kommunikationsform und Sicherungsmethode sie für den jeweiligen Verfahrensschritt für ausreichend oder erforderlich hält. Inwiefern z. B. die einfache E-Mail als Kommunikationsmittel tatsächlich zur Wahrung der Anforderungen genügt, muss jede Verwaltung verfahrensabhängig selbst prüfen. Kommt sie zu dem Schluss, dass dies nicht ausreicht, muss sie dann prüfen, welche Alternativen (z. B. Verschlüsselung, De-Mail, ePost oder Bürgerkonto) in Betracht kommen und wie diese implementiert werden können. Die Nutzung der herkömmlichen Schriftform oder ihrer gesetzlich bestimmten Ersatzformen bleibt immer möglich.

Zur Ermessenseinschätzung wird auf die „Handreichung zum Einsatz von Vertrauensmechanismen in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft" des IT-Planungsrats verwiesen. Diese stellt Richtlinien zur Ermittlung des erforderlichen Schutz- und Vertrauensniveaus einer Verwaltungsdienstleistung vor und definiert, welche Technologie bei welchem Schutzniveau erforderlich ist. Die einfache E-Mail ohne Verschlüsselung wird nur für Verfahren mit untergeordnetem Schutzniveau empfohlen. Schon bei einem normalen Schutzniveau sind Kommunikationswege vorgesehen, die größere Sicher-

36 BT-Drs. 18/10183, 66.
37 BT-Drs. 18/10183, 69.

heit bieten. Ob die Änderungen durch das Gesetz daher tatsächlich eine Arbeits- und Kommunikationserleichterung darstellen, hängt ganz entscheidend vom konkreten Verfahren ab sowie dem Willen der Behörden und deren Kommunikationspartnern.

Der Bundesgesetzgeber förderte durch diese Formerleichterung die Verwendung von nicht-qualifizierten Vertrauensdiensten, insbesondere fortgeschrittene Signaturen im Sinne von Art. 26 eIDAS-VO zur Verwendung in öffentlichen Diensten im Sinne von Art. 27 eIDAS-VO. Auch wird dadurch der Einsatz von elektronischen Siegeln grundsätzlich ermöglicht.

### *5. Blockchain*

Sowohl die Portalkommunikation als auch das Formerfordernis „oder elektronisch" bedürfen des Einsatzes von Technologien, die Authentizität und Integrität gewährleisten und somit auch Rechtssicherheit schaffen können. Grundsätzlich könnten dazu Vertrauensdienste zum Einsatz gebracht werden. Aber auch Technologien abseits der in der eIDAS-VO geregelten Vertrauensdienste können dazu genutzt werden. Eine solche Technologie könnte die Blockchain sein.

Längst ist die Blockchain mehr als nur die Technologie hinter der Kryptowährung Bitcoin. Die Technologie wird seit Jahren zugesagt, hochgradig potenziell geeignet zu sein, etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern.[38] Blockchain kann für verschiedene Anwendungen genutzt werden. Die zugrundeliegende Technologie sorgt dafür, dass auch über ein verteiltes System Transaktionen oder Aktionen der Teilnehmer eindeutig, einmalig, nachvollziehbar und belegbar sind.

#### *a) Technik*

Das kleinste Element einer Blockchain ist immer ein Block. Er besteht neben einem Index und einem Zeitstempel aus mindestens drei Komponenten: den eigentlichen Daten, dem Hash des Vorgängerblocks und einem sogenannten Proof of Work. Eine Blockchain ist eine Art Datenbank, in

38 *Schlatt/Schweizer/Urbach/Fridgen*, Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT), 2016, 1.

der Einträge in Blöcken gruppiert werden. Diese Blöcke sind in chronologischer Reihenfolge über eine kryptographische Signatur miteinander verknüpft.[39] Jeder Block enthält Aufzeichnungen valider Netzwerkaktivität seit dem Hinzufügen des letzten Blocks. Im Falle von Bitcoin umfasst dies beispielsweise die durchgeführten Transaktionen. Der Konsensmechanismus, mittels dessen die Netzknoten den Systemstatus koordinieren, wird als die grundlegende Innovation hinter Blockchain-Systemen angesehen.[40] Blockchains, wie z.B. auch Bitcoin, nutzen zwei fundamentale Konzepte der Kryptographie: digitalen Signaturen und kryptographische Hash-Funktionen.[41] Blockchains verwenden in der Regel eine asymmetrische Verschlüsselung sowohl zur Identifikation der Teilnehmer als auch zur Sicherung derer Aktionen.

### *b) Blockchain und eIDAS*

Eine der hervorstechendsten Eigenschaften der Blockchain ist ihre Robustheit gegen nachträgliche Änderungen einmal gespeicherter Daten. Deshalb kommt sie als Speichermedium überall da in Frage, wo Daten fortlaufend anfallen und manipulationssicher aufbewahrt werden müssen.

Eine Blockchain-Anwendung kann so organisiert sein, dass sich die Anwender nicht identifizieren müssen und sich die notwendigen Signaturen selbst erstellen. Es gibt aber auch verteilte, öffentliche Systeme, bei denen für die Teilnehmer eine Genehmigung und Identifizierung erforderlich ist. Auch gibt es private, verteilte Systeme, bei denen für die Teilnahmen eine Genehmigung erforderlich ist und zentral verwaltete Blockchain-Register.

Grundsätzlich kann deswegen der Anwendungsbereich für die eIDAS-VO auch bei Blockchain eröffnet sein. Entweder kommen zu deren Realisierung Vertrauensdienste im Sinne der eIDAS-VO zur Anwendung oder die Blockchain-Technologie wird eingesetzt, um damit einen Vertrauensdienst anzubieten.[42] So sind öffentliche Blockchain-Anwendungen, die in irgendeiner Art und Weise Nutzern elektronische Signaturen zur Verfü-

---

39 *Walport*, Distributed Ledger Technology: beyond block chain, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 2015.

40 *Schlatt/Schweizer/Urbach/Fridgen* (Fn. 38), 9.

41 *Böhme/Christin/Edelman/Moore*, Bitcoin: Economics, Technology, and Governance, The Journal of Economic Perspectives 2015, 213.

42 *Brisch/Brisch*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 50. Ed., München 2019, Teil 13.3, Rn. 134-137.

gung stellen, Vertrauensdienste im Sinne der eIDAS, unabhängig davon, ob eine Identifizierung erfolgt.[43] Blockchain-Anwendungen, die in irgendeiner Art und Weise den Ursprung und die Unversehrtheit elektronischer Daten für ein Unternehmen sicherstellen sollen, können elektronische Siegel im Sinne der eIDAS sein. Blockchain-Anwendungen, die in irgendeiner Art und Weise elektronische Daten mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese Daten zu diesem Zeitpunkt vorhanden waren, können elektronische Zeitstempel im Sinne der eIDAS sein.[44] Die Anbieter solcher Blockchaindienste sind Vertrauensdiensteanbieter. Die Dienstanbieter unterliegen als einfache oder fortgeschrittene Vertrauensdienstanbieter einer ex post Aufsicht durch die Bundesnetzagentur.

Die Blockchain gilt als technisch sehr sicher, weil Manipulationen durch Prüfung der verwendeten digitalen Signaturen und Hashes aufgedeckt werden können. Soweit sie aber ohne qualifizierte elektronische Signaturen, Siegeln oder Zeitstempel betrieben wird, kann sich ihr Verwender nicht auf die Beweiserleichterungen nach der eIDAS-VO und § 371a Abs. 1 ZPO berufen. In der Gerichtspraxis obläge dem Gericht, einen Beweis durch Augenschein nach § 371 ZPO zu erheben und ihn nach § 286 ZPO frei zu würdigen.[45] Als elektronischem Dokument darf der Blockchain aber gemäß Art. 46 eIDAS-VO weder die Rechtswirkung und noch die Zulässigkeit als Beweismittel in Gerichtsverfahren allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt.

## *V. Fazit*

Schon die kursorische Prüfung zeigt, dass im elektronischen Rechts- und Geschäftsverkehr aufgrund unionaler und nationaler Ko-Regulierung, ein schwer zu überblickendes und verflochtenes Regelnetz entstanden ist. Dies wird einerseits durch technologische Entwicklungen, wie Blockchain, und andererseits durch neue Anwendungsfälle, wie Kundenportalpostfächer, noch verwobener. Die eIDAS-VO und deren Regeln zu Vertrauensdiensten sitzt in diesem Netz wie eine Spinne. Aber diese hält nicht alle Fäden in der Hand.

---

43 Z.B. http://www.scytale.tech.
44 Z.B. https://timebeat.com.
45 *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278, 3283.

Nicht alle Vertrauensdienste unterfallen vollumfänglich der eIDAS-VO. Und auch außerhalb der eIDAS-VO oder gar nicht geregelte Dienste müssen keine Bärendienste sein. Auch sie können Vertrauen generieren und faktische Sicherheit und Kontrollmöglichkeiten schaffen. Das gilt für gesetzlich geregelte Dienste wie DeMail ebenso wie für Dienste, die Blockchain verwenden. Abseits gesetzlicher Regelungen und gerichtlicher Erfahrungswerte müssen die Anwender jedoch ihrerseits einen erhöhten Auswahl- und Überprüfungsaufwand betreiben. Oder sich auf einen Tanz mit dem Bären einlassen.