



Juli 2011 Seiten 289–336

 **Stbg** 7/2011

# Die Steuerberatung

ORGAN DES DEUTSCHEN STEUERBERATERVERBANDES E.V. BERLIN  
WWW.DSTV.DE

Mitgliederversammlungen des DStV und des DStI in Trier

## STEUERRECHT

- Staats | Änderungen in den Erklärungsvordrucken 2010 für Körperschaften | 293 |
- Kirmes | Liberalisierung von Sicherungsvorschriften für E-Rechnungen | 299 |
- Wenzel | Aktuelle Entwicklung zur eingetragenen Lebenspartnerschaft | 314 |
- Nebe | Bekanntgabe eines Erbschaftsteuerbescheids an Testamentsvollstrecker | 317 |

## BILANZRECHT

- Eggert | Latente Steuern nach dem BilMoG – bei allen Kaufleuten? | 318 |



Diese Verordnung wurde durch die SteuerHBekV vom 25. 9. 2009<sup>40</sup> erlassen. Bei Erfüllung der übrigen Voraussetzungen findet sie für Steuerbefreiungen nach § 8b KStG nach §§ 4, 6 SteuerHBekV erstmals Anwendung für den Veranlagungszeitraum 2010 bzw. Gewinnausschüttungen, die nach dem 31. 12. 2009 zufließen.

V. Ausblick

Der Finanzausschuss des Bundestages hat im Rahmen des Gesetzgebungsverfahrens zum Steuervereinfachungsgesetz vorgeschlagen, abweichend von § 27 Abs. 2 Satz 4 KStG auf die Feststellungserklärung zum steuerlichen Einlagekonto gem. § 27 KStG (s. Abschn. II.5 bzw. II.6) zu verzichten, sofern im Wirtschaftsjahr keine Änderungen eingetreten sind.

Der DStV<sup>41</sup> hat in seiner Stellungnahme an den Finanzausschuss jedoch dafür plädiert, aus praktischen Gründen an der Erklärungspflicht festzuhalten. Zum einen sei der Aufwand dafür gering, wenn lediglich die Vorjahres-

werte übernommen zu werden bräuchten. Zum anderen diene die Erklärung auch der Dokumentation der steuerlichen Pflichten. Ferner sei zu bedenken, dass in der Finanzverwaltung ab einem bestimmten Zeitpunkt die Unterlagen nicht mehr ohne Weiteres zugänglich seien. Würde die Körperschaft nach langjähriger Unterbrechung wieder eine Feststellungserklärung abgeben, wäre ein Abgleich mit früheren Erklärungen seitens des Finanzamts allenfalls mit erheblichem Aufwand möglich.

Die Bundesregierung hat den Vorschlag ebenfalls abgelehnt. Es bestehen jedoch Überlegungen, zwar an der Erklärungspflicht festzuhalten, die maßgebenden Vordrucke jedoch dahingehend zu ergänzen, das durch Ankreuzen erklärt werden kann, dass im Wirtschaftsjahr keine Änderungen im steuerlichen Einlagekonto erfolgt sind, wodurch sich das weitere Ausfüllen der Erklärung erübrigen würde.

40 SteuerHBekV vom 25. 9. 2009, BGBl. I 2009 S. 3046 = BStBl I 2009 S. 1146.

41 DStV-Eingabe S 7/11 vom 6. 5. 2011, www.dstv.de.

## Zum Stand der Liberalisierung von Sicherungsvorschriften für Elektronische Rechnungen – Nachschau auf einen Pyrrhussieg der „Ent-Bürokraten“

Dipl.-iur. Raoul Kirmes (CISA), Berlin<sup>1</sup>

Der nachfolgende Aufsatz analysiert die Änderungen der Vorschriften für Elektronische Rechnungen (E-Rechnungen) durch die Richtlinie 45/2010 EU<sup>2</sup> vom 13. 7. 2010, welche die Mehrwertsteuer-Systemrichtlinie EG 112/2006 vom 28. 11. 2006<sup>3</sup> mit Wirkung zum 13. 7. 2010 änderte. Die Umsetzung in deutsches Recht soll gem. Art. 16 Abs. 3 des Steuervereinfachungsgesetzes 2011 mit Wirkung zum 1. 7. 2011 durch Anpassung von § 14 Abs. 1, 3 und § 14b Abs. 1 Satz 2 sowie § 27 Abs. 18 UStG n. F. erfolgen.

I. Einleitung

Die im Folgenden besprochenen Vorschriften haben durch ihren fiskalischen Zweck und ihren supranationalen Ursprung eine kaum zu unterschätzende, branchenübergreifende Bedeutung für die **gesamte IT-Sicherheitspolitik in Unternehmen**. Wie es der Leiter des Indirect Tax Committee der TEI,<sup>4</sup> *Jean-Daniel Rouvinez*, treffend formulierte: **Die steuerrechtliche Wirkung ist lediglich die Spitze des „Bedeutungseisbergs“ der E-Rechnung**.<sup>5</sup> Die gesetzlichen Vorschriften für den elektronischen Rechnungsversand adressieren verschiedene klassische IT-Sicherheitsprobleme in Unternehmen und markieren damit auch den gesetzlichen Bewertungsmaß-

stab hinsichtlich der Eignung und Akzeptanz verschiedener möglicher zu ergreifender Sicherheitsmaßnahmen für diese Probleme.

Die Änderungsrichtlinie 45/2010 EU ist zudem aus zwei weiteren Gesichtspunkten besonders interessant. Zum einen beinhalten die geänderten Vorschriften neben den bekannten technischen Sicherheitsmaßnahmen für

1 Dipl. iur. *Raoul Kirmes*, (CISA), QMA-TÜV ist Vorstand des Software-Industrieverbandes Elektronischer Rechtsverkehr (SIV-ERV) und bei der VISUS-Wirtschaftsprüfungsgesellschaft (Berlin) zuständig für IT-Sicherheitsmanagementsysteme, Rechtsinformatik, Governance, Risk & Compliance Management.

2 ABl.EU 2010 Nr. L 198/1.

3 ABl.EG 2006 Nr. L 347/1.

4 Die Abkürzung „TEI“ steht für die Firmierung des Weltverbandes der Steuerjurist:innen „Tax Executives Institute (Inc.)“. Die TEI stellt sich selbst wie folgt dar: „TEI was founded in June of 1944 by a group of 15 prominent corporate tax executives in New York City. Today the institute has nearly 7,000 members, aligned in 54 separate chapters, and representing over 3,200 leading businesses in the United States, Canada, Europe and Asia“, [www.tei.org](http://www.tei.org) (Stand 6. 2. 2011).

5 Im Text durch den Verfasser sinngemäß wiedergegeben, der genaue Wortlaut war: „die Rechnung als Eisberg, bei dem die VAT die Spitze bildet, der kommerzielle Wert des eigentlichen Rechnungsbetrags, der unter Wasser liegt, aber um den geschätzten Faktor 5 den Wert der VAT übersteigt. Jede Optimierung der Abwicklung des Rechnungsbetrags hat demnach wesentlich größere Auswirkungen auf die Unternehmen als die bloße Fokussierung auf die VAT“, zitiert aus dem Bericht zur „Electronic Invoicing in Europe-Konferenz“ in Madrid vom 27.–28. 4. 2010; Bericht der intarsys Consulting GmbH, Karlsruhe, mit Verweis auf: [ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm](http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm) (Stand 15. 2. 2011).

E-Rechnungen (qualifizierte E-Signatur<sup>6</sup> und EDI<sup>7</sup>) auch einen **neuen Tatbestand für organisatorische Sicherheitsmaßnahmen**, den sog. „**verlässlichen Prüfpfad**“,<sup>8</sup> dessen Tatbestandsmerkmale nachfolgend im Einzelnen zu ermitteln sein werden. Zum anderen war die Änderung der Richtlinie EG 112/2006 politisch heiß umkämpft, weil die E-Rechnung in den Fokus der „Entbürokratisierung“ gekommen war.<sup>9</sup> Hier gilt es, Resümee zu ziehen und zu bewerten, ob die Änderungen auch in der Praxis tatsächlich eine Vereinfachung für die Unternehmen zu bewirken vermögen.

## II. Umsetzung in deutsches Recht

Bereits am 20.12.2010 legte das BMF den Referententwurf<sup>10</sup> für das Steuervereinfachungsgesetz 2011 (StVereinfG 2011) vor, mit dem bereits eine Umsetzung der Richtlinie 45/2010 EU in deutsches Recht erfolgt. Die hier diskutierten Änderungen des UStG (Art. 5) sollen nach Art. 16 Abs. 3 StVereinfG 2011 bereits am 1. 7. 2011 in Kraft treten. Der Gesetzgeber will also die Umsetzungsfrist<sup>11</sup> in Bezug auf die Regelungen zur E-Rechnung nicht ausnutzen, sondern sehr schnell eine Anpassung des nationalen Rechts vornehmen. Hintergrund der Eile sind offensichtlich die mit der Änderung vorgerechneten Bürokratiekostenentlastungen von abenteuerlichen 4 Mrd. €, von denen allein 3,3 Mrd. € auf eine angebliche Erleichterung bei der Aufbewahrung von Rechnungen in § 14b UStG entfallen sollen.<sup>12</sup> Allerdings wurden die Vorschriften in § 14b UStG verschärft und nicht erleichtert.<sup>13</sup> Es bleibt offen, wie das zusammenpasst.

Am 18. 4. 2011 hat das BMF dann zusätzlich einen Fragen-und-Antworten-Katalog (FAQ) zu den Änderungen veröffentlicht.<sup>14</sup> Leider ist dieses Dokument von handwerklichen Unzulänglichkeiten<sup>15</sup> geprägt und zudem offensichtlich politisch eingefärbt.<sup>16</sup> Insbesondere lässt das BMF, sofern es überhaupt an einigen wenigen Stellen über die bloße Wiederholung des Richtlinien textes hinausgeht, jedwede europarechtliche Anbindung vermissen.<sup>17</sup> Wichtige Fragen, die insbesondere die Kohärenz mit anderen Verlautbarungen des BMF<sup>18</sup> betreffen und für deren Klarstellung die FAQs gut hätten genutzt werden können, werden nicht einmal angesprochen. Einiges werde ich noch in VIII. aufzeigen.<sup>19</sup>

## III. Motivation und Zweck der Änderungsrichtlinie

### 1. Zielstellungen der Änderungsrichtlinie

Der europäische Gesetzgeber verfolgt mit Anpassung der Vorschriften für den elektronischen Rechnungsversand drei zentrale Vorhaben:

#### a) Stärkung der Betrugsprävention/Förderung der E-Rechnung

„Bestimmte Vorschriften über die obligatorischen Rechnungsangaben **sollten so geändert werden, dass sie**

**eine bessere Steuerkontrolle gewährleisten, (...)** und die elektronische Rechnungsstellung fördern.“<sup>20</sup>

Der deutsche Gesetzgeber formuliert in der Begründung zur Änderung des § 27b Abs. 2 Satz 2 und 3 UStG n. F.:

„Die Reduzierung der Anforderungen an eine elektronische Rechnung (...) kann nicht einseitig zu Lasten einer

6 I.S.v. § 2 Nr. 3 SigG auf Grundlage der RL 1999/93/EG.  
 7 EDI-Verfahren gem. KOM-Empfehlung 94/820/EG.  
 8 Das Verfahren wird von den Befürwortern auch als „Dritter Weg“ zur Sicherung neben Signatur und EDI beschrieben, *Groß/Lamm*, Elektronische Rechnung künftig einfacher?, Anm. zum Entwurf für ein Steuervereinfachungsgesetz 2011 vom 2. 2. 2011, www.psp.eu.  
 9 Beispielhaft hier nur z. B.: Deutschlandradio, Interview mit *Edmund Stoiber*, „Kampf gegen Windmühlen und das Ringen um Bürokratieabbau in Brüssel“, in dem die Streichung der elektronischen Signatur auf die Agenda der Entbürokratisierung durch die sog. „Stoiber-Group“ gesetzt wurde; Bericht über die Ergebnisse der öffentlichen Konsultation zum Thema: „MwSt – Überprüfung bestehender Rechtsvorschriften zur Fakturierung“ (TAXUD/D (2008) / 25115) vom November 2008. Vorangegangen war der „Final Report vom 3. 11. 2008“ der Wirtschaftsprüfungsgesellschaft PWC; dazu folgend die Stellungnahme an die Europäische Kommission des Software Industrieverbandes elektronischer Rechtsverkehr (SIV-ERV e. V.) zur Änderung der RL EG 112/2006 vom Januar 2009 (*Kirmes/Balfanz*), welcher den Vorschlag der Kommission kommentiert; darauf folgte der Bericht der Expert Group e-Invoicing (EG) zum Vorschlag für eine Richtlinie zur Änderung der RL 2006/112/EG über das gemeinsame Mehrwertsteuersystem hinsichtlich der Rechnungsstellungsverordnungen, der nochmals 87 kontroverse Stellungnahmen aus diversen Verbänden und Staaten hervorrief, hier nur exemplarisch: [Pro-Sicherheit] Stellungnahme an die Europäische Kommission des Software Industrieverbandes elektronischer Rechtsverkehr (SIV-ERV e. V.) zum Bericht KOM (2009) 21, Version: 1.5 vom Januar 2010 (*Kirmes/Gass*); Stellungnahme des VOI – Verband Organisations- und Informationssysteme e. V. zum Report der EU elnvoice Experten Gruppe vom November 2009 (*Berndt*); Stellungnahme des Berufsverbandes der Trustcenterbetreiber (T7 e. V.) zum Vorschlag für eine Richtlinie zur Änderung der RL 2006/112/EG über das gemeinsame Mehrwertsteuersystem hinsichtlich der Rechnungsstellungsverordnungen, KOM(2009) 21; [Contra-Sicherheit] *Fritsch* (Mitglied der High Level Group of Independent Stakeholders on Administrative Burdens), zitiert aus dem Bericht der „Electronic Invoicing in Europe Konferenz“ in Madrid vom 27.–28. 4. 2010; vgl. auch Empfehlungen der Ausschüsse EU – Fz. – Wi. zur 863. Sitzung des Bundesrates am 6. 11. 2009, BR-Drucks. 157/1/09.  
 10 Der Gesetzentwurf wurde sodann am 2. 2. 2011 vom Bundeskabinett beschlossen, vgl. Entwurf eines StVereinfG 2011, BT-Drucks. 17/5125.  
 11 Deutschland hatte nach Art. 2 der RL 2010/45/EU eine Umsetzungsfrist bis zum 31. 12. 2012.  
 12 Gesetzesbegründung zum StVereinfG 2011, BT-Drucks. 17/5125 S. 46 Nr. 15, 16, 17 (4 Mrd. € setzten sich wie folgt zusammen: § 14 Abs. 1 UStG – 255 657 T€; § 14 Abs. 3 UStG – 487 125 T€; § 14b UStG – 3 305 393 T€).  
 13 Dazu unter V. im Einzelnen.  
 14 Veröffentlichungen zu Steuerarten vom 19. 4. 2011, Frage-Antwort-Katalog zur Vereinfachung der elektronischen Rechnungsstellung zum 1. 7. 2011 durch Art. 5 StVereinfG 2011, IV D 2 – S 7287-a/09/10004, www.bmf.de (Stand 22. 4. 2011).  
 15 So ist schon ungewöhnlich, dass das BMF sich vorab durch FAQ's zu einem Gesetz äußert, das es zu diesem Zeitpunkt noch nicht gab. Zitat: „Bislang liegt hierzu lediglich ein Gesetzentwurf der Bundesregierung vor, der sich zurzeit im parlamentarischen Verfahren befindet. Erst Bundestag und Bundesrat werden über die endgültige Ausgestaltung der gesetzlichen Regelungen entscheiden.“ Insofern ist der politische Druck, „frohe Botschaften“ zu verkünden, nicht zu übersehen.  
 16 Man betont über Gebühr die „Vereinfachung“, die jedoch, wie sich aus dem Folgenden noch ergeben wird, nicht gegeben ist.  
 17 Die Auslegungsprärogative für europäische Richtlinien liegt beim EuGH und nicht beim BMF, insofern ist es eher kontraproduktiv, wenn eine nationale Behörde versucht, den Vorschriften eine eigene nationale Färbung zu geben. Genau das war die Ursache für die Kompatibilitätsprobleme innerhalb der EU. Notwendig ist ein möglichst gleicher Vollzug der Regelungen in allen europäischen Staaten.  
 18 BMF vom 29. 1. 2004, IV B 7 – S 7280 – 19/04, BStBl I 2004 S. 258, insb. Rz. 70; vgl. auch VIII.  
 19 Kritisch *Groß/Lamm*, Elektronische Rechnungen – praktische Hinweise zur Neuregelung ab dem 1. 7. 2011, BC – Zeitschrift für Rechnungswesen und Controlling, Heft 6/2011 S. 244.  
 20 Einführung zur RL 2010/45/EU des Rates vom 13. 7. 2010 Nr. 7.

effektiven Steuerbetrugsbekämpfung gehen und zu Risiken für die Haushalte von Bund und Ländern führen.“<sup>21</sup>

Eine Liberalisierung durch **Absenkung** des **Sicherheitsniveaus** kann somit als Zielstellung **sicher ausgeschlossen** werden. Alle folgenden Überlegungen müssen beachten, dass eine Absenkung des Sicherheitsniveaus zum Status quo nicht beabsichtigt ist.

**b) Technikneutrale Anpassung der Vorschriften**

Der Richtliniengeber beabsichtigt vielmehr, die zulässigen Sicherungsverfahren zu liberalisieren, ohne das Sicherheitsniveau als solches abzusenken. Die Kommission schreibt dazu in den Erläuterungen: „Die Echtheit und Unversehrtheit von elektronischen Rechnungen lassen sich (...) durch Nutzung bestimmter vorhandener Technologien, wie beispielsweise elektronischen Datenaustausch (EDI) und fortgeschrittene elektronische Signaturen, sicherstellen. Da es jedoch auch **andere Technologien** gibt, sollte den Stpfl. nicht die Nutzung einer speziellen Technologie der elektronischen Rechnungsstellung vorgeschrieben werden.“<sup>22</sup>

Damit wurde der Forderung nachgekommen, eine technikneutrale Regelung zu schaffen, die es auch in Zukunft ermöglicht, auf technologische Änderungen angemessen zu reagieren und nicht länger innovative Verfahren von vornherein auszuschließen. Dieses Vorhaben muss in jeder Hinsicht Unterstützung finden, weil es schlicht keine legitime Begründung für die Bevorzugung bestimmter Verfahren gibt.

**c) Gleichbehandlung der elektronischen Verfahren**

Als dritte Zielstellung hat sich der Richtliniengeber vorgenommen, zukünftig dafür zu sorgen, dass bei der Bewertung elektronischer Systeme keine höheren Maßstäbe angelegt werden als in der physischen Welt. „Rechnungen auf Papier und elektronische Rechnungen sollten gleichbehandelt werden (...).“<sup>23</sup>

Damit soll den in der Praxis vorzufindenden Übertreibungen bei der Bewertung von Sicherheitsanforderungen an IT-Systeme Einhalt geboten werden. Diese Ermessensbegrenzung der Finanzverwaltung ist zu begrüßen, darf jedoch nicht darüber hinwegtäuschen, dass elektronische Systeme ganz eigene – eben typisch elektronische – Gefahren und Probleme in der Umsetzung von Sicherheit mit sich bringen. Soweit solche **sachlichen Unterschiede** zwischen Papier und elektronischer Welt bestehen und besondere Maßnahmen erfordern, sind diese auch weiterhin zu ergreifen. Ein falsch verstandenes Gleichbehandlungsargument wird nicht tragen.

Eine **Vereinfachung** der technischen Vorschriften für die Absicherung elektronischer Rechnungen war offenbar im Ergebnis des Konsultationsverfahrens **nicht mehr beabsichtigt**.

In der Erläuterung heißt es dazu: „Die Kommission hat gem. Art. 237 jener Richtlinie einen Bericht vorgelegt, in dem vor dem **Hintergrund der technologischen Entwicklungen** bestimmte Schwierigkeiten der elektronischen Rechnungsstellung beschrieben **und einige andere Bereiche** genannt werden, **in denen die MwSt-Vorschriften vereinfacht werden sollten**, um die Funktionsweise des Binnenmarkts zu verbessern.“<sup>24</sup>

**IV. Die neue Regelungssystematik der Richtlinie 112/2006 EG**

**1. Das neue Eigenverantwortungsprinzip**

Mit der Neuformulierung von Art. 233 Abs.1 Satz 2<sup>25</sup> vollzieht die Kommission tatsächlich einen systematischen Paradigmenwechsel. Bislang hatte der Gesetzgeber selbst durch abschließende Bestimmung im Gesetzestext eine Auswahl der nach seiner Ansicht geeigneten technischen Sicherungsmittel getroffen und damit auch das inhärente Technikrisiko für diese Auswahl übernommen.<sup>26</sup> In der neuen Formulierung **verlagert er dieses Technikrisiko** nun auf die **Unternehmen** und legt es damit in ihre „Eigenverantwortung“, eine geeignete Auswahl zu treffen. In Art. 233 Abs.1 Satz 2 heißt es nun:

„Jeder Steuerpflichtige legt fest, in welcher Weise die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet werden können.“

Allerdings ist dies – entgegen der teilweise euphorischen Reaktion aus den Reihen der „Entbürokraten“<sup>27</sup> – sicher kein Anlass zu übermäßiger Freude, folgt doch daraus, dass die schwierige und kostenträchtige Evaluierung und Bewertung von IT-Sicherheitssystemen nun allein in der Verantwortung der Unternehmen liegt. Nutzt der Rechnungsaussteller eines der ausdrücklich in Art. 233 Abs. 2 Buchst. a) und b) genannten Verfahren (Signatur oder EDI), verbleibt zwar eine gesetzliche Konformitätsvermutung,<sup>28</sup> was die Kosten der Entscheidungsfindung und der Dokumentation einer sorgfältigen Auswahl deut-

21 Entwurf eines StVereinfG 2011, BT-Drucks. 17/5125 S. 85 zu Nr. 4.  
 22 Einführung zur RL 2010/45/EU des Rates vom 13. 7. 2010 Nr. 11.  
 23 Einführung zur RL 2010/45/EU des Rates vom 13. 7. 2010 Nr. 8.  
 24 Einführung zur RL 2010/45/EU des Rates vom 13. 7. 2010 Nr. 1.  
 25 Art.-Angaben ohne nähere Bezeichnung beziehen sich immer auf die RL 112/2006 EG, ABIEG 2006 Nr. L 347/1, in der aktuellen Fassung der RL 45/2010 EU, ABIEU 2010 Nr. L 198/1.  
 26 Die Kehrseite war selbstverständlich eine Bevorzugung dieser technischen Verfahren gegenüber Anderen durch Erhebung zu einem de-jure-Standard. Dieses Problem wurde zu Recht kritisiert. Der neue Pluralismus der technischen Möglichkeiten wird jedoch zunächst recht teuer durch die volle Risikoübernahme der Unternehmen erkauft; erst wenn ein Markt neuer Alternativverfahren entstehen würde, könnten sich diese Mehrkosten wieder rentieren, sofern es möglich ist, den Preis für den Versand elektronischer Dokumente noch weiter zu senken. In Anbetracht des aktuellen Preises für elektronische Rechnungen zwischen 5 und 10 Cent darf das bezweifelt werden.  
 27 Vgl. diverse Veröffentlichungen der Österreichischen Wirtschaftskammer im Internet.  
 28 Vgl. § 292 Satz 1 ZPO: „Stellt das Gesetz für das Vorhandensein einer Tatsache eine Vermutung auf, so ist der Beweis des Gegenteils zulässig, sofern nicht das Gesetz ein anderes vorschreibt“.

lich reduziert. Festzuhalten ist jedoch, dass auch diese Verfahren nun nicht mehr per se von Gesetzes wegen als sicher gelten, sondern „nur“ eine gesetzliche Vermutung für ihre Sicherheit spricht.<sup>29</sup> All jene Unternehmen, die bereits in diese Technik investiert haben, wurden also im Vergleich zur Rechtslage vor der Änderung etwas schlechter gestellt. Auch sie trifft zukünftig eine Überwachungspflicht, ob diese Verfahren **noch** als sicher gelten dürfen, was naturgemäß einer ständigen Entwicklung unterliegt. Die mit der Auswahl eines geeigneten Verfahrens verbundenen Kosten<sup>30</sup> werden weder durch die Kommission thematisiert noch in der Gesetzesbegründung zum StVereinfG 2011 erkannt.<sup>31</sup>

## 2. Die Schutzrichtung der formulierten Sicherheitsziele

Wichtig für eine zutreffende Anwendung der Sicherheitsvorschriften für E-Rechnungen ist es, ein Verständnis für die bezweckte Schutzrichtung zu entwickeln. Die Regelungen dienen nicht primär dem Schutz der Unternehmen (als Aussteller oder Empfänger von Rechnungen) vor Betrug, sondern sie schützen das Umsatzsteueraufkommen in der EU als Ganzes.<sup>32</sup> Diese Bemerkung erscheint hier notwendig, da in der Diskussion um den Sinn von Sicherungsmaßnahmen für E-Rechnungen und zuletzt auch wieder durch die FAQ des BMF<sup>33</sup> fehlerhaft das Argument vorgebracht wurde, [sinngemäß] „der Unternehmer würde schon wissen, ob eine Rechnung zu bezahlen sei.“ Die Schutzrichtung zielt jedoch nicht auf die Vermögensinteressen der Unternehmen ab, sondern dient primär dem Zweck einer effektiven Bekämpfung des Umsatzsteuerbetrugs. Es geht also, wenn man so will, um „Innentäter“,<sup>34</sup> denen das Abstreiten der „Ausstellung“<sup>35</sup> einer E-Rechnung oder die Fakturierung von Scheinleistungen erschwert werden soll. Nur reflexartig bieten die Vorschriften auch Schutz für das lautere Unternehmen vor gefälschten Rechnungen in seinem Namen. Dieser Zweck wird in der Diskussion um Vereinfachungen, aber auch bei der Auslegung der Vorschriften gerne ausgeblendet. Anders als bei der papiergebundenen Post ist der Versand von Dokumenten (Rechnungen) über das Internet kostenlos, so dass die Gefahr darauf aufbauender Betrugsmodelle nicht unterschätzt werden sollte. Die Statistik<sup>36</sup> erfolgreicher Phishing-Angriffe verdeutlicht, dass es sehr wohl möglich ist, allein mit dem Anschein der Echtheit erheblichen Schaden im Internet zu verursachen. Für die Praxis der Abschlussprüfer<sup>37</sup> stellt sich zudem das Problem der Abwehr doloser Handlungen. Die Beurteilung der Beweiskraft einer Buchhaltung (§§ 238, 239 und 257 HGB; § 158 AO) wird extrem erschwert, wenn die elektronischen Belege nicht unabstreitbar<sup>38</sup> einem Urheber zugeordnet werden können. Die größten Bilanzskandale in den zurückliegenden Jahren basierten alle auch auf Belegfälschungen **im** Unternehmen, die Fiskus und Aufsichtsbehörden über die tatsächliche Situation der Unternehmen täuschten.<sup>39</sup> Die Evidenz einer Prüfung baut im Bereich der Posten<sup>40</sup> auf der Annahme auf, dass es keine Buchung ohne Beleg geben darf (Beleg-

grundsatz).<sup>41</sup> Die Integrität und Authentizität von Belegen wird zwar durch Strafvorschriften geschützt,<sup>42</sup> sind diese jedoch nicht mehr sicher einem Urheber zuweisbar, oder lässt sich ihre Manipulation forensisch nicht gerichtsfest belegen, laufen auch die Strafvorschriften ins Leere. Der dolos Handelnde kann sich jeglichem Sanktionsgefüge entziehen. Nicht umsonst verlangen alle Empfehlungen<sup>43</sup>

- 29 Insbesondere die in Deutschland ungewöhnlich starke Privilegierung der qualifizierten elektronischen Signatur durch § 371a ZPO i. V. m. § 2 Nr. 3 SigG führt für die Praxis in Deutschland auch weiterhin zu einer de facto gesetzlich garantierten Sicherheit. Diesen Vorzug kann freilich das EDI-Verfahren nicht für sich in Anspruch nehmen, so dass auch in diesem Bereich zukünftig mehr Aufwand zum Nachweis der Sicherheit zu treiben sein wird.
- 30 Gemeint sind die Kosten für die Evaluierung und Prüfung von IT-Sicherheitssystemen. Dabei ist zu beachten, dass im technischen Sicherheitsrecht durch internationale Abkommen die Anerkennung sicherer IT-Systeme einem weitgehend verbindlichen Verfahren folgt (Common Criteria und ISO/IEC 15408); auch die Zertifikate nach z. B. IDW-PS 880, 951 oder ISO/IEC 27001 fordern regelmäßig erhebliche finanzielle Aufwendungen, bestenfalls nur bei den Systemherstellern.
- 31 Vgl. Referentenentwurf zum Steuervereinfachungsgesetz 2011 vom 20. 12. 2010. Der Gesetzentwurf führt unter „E. Sonstige Kosten“ aus: „Mögliche einmalige Anpassungskosten der Beteiligten an die neue Rechtslage werden von den zu erwartenden dauerhaften Einsparungen bei den Bürokratiekosten insgesamt weit übertroffen“. Ich habe meine Zweifel, ob dies bei Anwendung des Audit-Trail tatsächlich gewährleistet ist.
- 32 Vgl. Vorschlag für eine Richtlinie des Rates zur Änderung der RL 2006/112/EG über das gemeinsame Mehrwertsteuersystem hinsichtlich der Rechnungsstellungsvorschriften vom 28. 1. 2009, KOM (2009) 21: „Ein wichtiger Aspekt neben der Vereinfachung, Harmonisierung und Modernisierung der Vorschriften ist die **Bekämpfung des MwSt-Betrugs**. In diesem Bereich wurde viel getan, und etwaige Änderungen der Rechnungsstellungsvorschriften dürfen die Ergebnisse dieser Arbeit nicht aufs Spiel setzen, sondern sollten vielmehr darauf abzielen, sie zu ergänzen.“
- 33 Jedenfalls drängt sich durch die Formulierung der Kontrollschritte der Eindruck auf, dass die Möglichkeit eines Umsatzsteuer-Karussells, in dem ohnehin nur Scheinleistungen fakturiert werden, in den Gedanken gar nicht vorkommt.
- 34 „Innen“ i. S. v. innerhalb einer Betrugs- oder Hinterziehungskonstellation.
- 35 Sehr lehrreich dazu die jüngste Entscheidung des BFH vom 17. 2. 2011, VR 39/09, DStR 2011 S. 969.
- 36 Vgl. Polizeiliche Kriminalstatistik 2009, BKA-Statistik, Kriminalistisches Institut Wiesbaden, Fachbereich KI 12, dort die Delikts-Nr. 517500 Computerbetrug § 263a StGB, 5163 Betrug mittels rechtswidrig erlangter Debitkarten mit PIN, 5179 Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten; alternativ und international ausgerichtet der monatliche Spam- und Phishing-Report auf <http://www.symantec.com>.
- 37 Die Verschärfung der Haftungsregelungen für die Abschlussprüfer und die erhebliche Ausweitung ihrer Aufgaben zur Bekämpfung von Betrug (Fraud) und Korruption werden zu einer deutlich schärferen Kontrolle elektronischer Verfahren führen, vgl. dazu das erstklassige Werk von *Melcher*, *Aufdeckung wirtschaftskrimineller Handlungen durch Abschlussprüfer*, 2009.
- 38 Die Nicht-Abstreitbarkeitsfunktion (non reputation) ist ein wesentlicher Vertrauensanker für die Absicherung verbindlicher elektronischer Kommunikation, vgl. dazu auch das Vorgehen des Gesetzgebers im Gesetzgebungsverfahren zum De-Mail-Gesetz, BT-Drucks. 17/3630 vom 8. 11. 2010; auch hier ist der entscheidende Vertrauensanker die sichere Erstidentifikation, verbunden mit der unabstreitbaren Dienstenutzung.
- 39 Vgl. dazu *Peemöller/Hofmann*, *Bilanzskandale*, S. 1 ff.
- 40 Gemeint sind alle Prüfaussagen bezogen auf das Zahlenwerk (Posten) der Bilanz, GuV, Anhang, Lagebericht.
- 41 Vgl. IDW RS FAIT 5.1 Tz. 29, „Die in § 238 Abs. 1 HGB geforderte Nachvollziehbarkeit der Buchführung vom Urbeleg zum Abschluss und vice versa setzt voraus, dass jede Buchung und ihre Berechtigung durch einen Beleg nachgewiesen wird (Grundsatz der Belegbarkeit). Sie ist die Grundvoraussetzung für die Beweiskraft der Buchführung.“
- 42 Die Existenz dieses Problems wird auch schon eindrucksvoll durch die Vielzahl von einschlägigen Strafvorschriften des StGB belegt, vgl. § 267 Urkundenfälschung; § 268 Fälschung technischer Aufzeichnungen, § 269 Fälschung beweiserheblicher Daten, § 270 Täuschung im Rechtsverkehr bei Datenverarbeitung, § 274 Urkundenunterdrückung, § 303a Datenveränderung, § 303b Computersabotage.
- 43 Vgl. IDW RS FAIT 5.3 Tz. 39; IDW RS FAIT Anhang 1, Nr. 2.1, Tz. 7; ebenso auch die Standards in Cobit 4.1 und folgende Versionen.

der prüfenden Berufe (IDW,<sup>44</sup> ISACA<sup>45</sup>) für die Abwicklung von elektronischen Transaktionen entsprechende Sicherungen. Nichts anderes gilt deshalb für die E-Rechnung. Selbst wenn man unterstellen würde, der Vorsteuerabzug setzte diese Anforderungen nicht mehr voraus (was nicht der Fall ist), so würde sich das Problem für die Unternehmen nur aus dem Regime der Umsatzsteuer auf das Regime des HGB verlagern. In jedem Fall würde die Verbuchung eines originär elektronischen Belegs Sicherheitsmaßnahmen erfordern, die eine Revisionsfestigkeit gewährleisten.

### 3. Schlussfolgerungen für die Auslegung der Vorschriften

Der Gesetzgeber hat sich entschieden, zukünftig einen sicherheitstechnischen Lösungspluralismus zuzulassen. Dazu musste er seine Gesetzgebungstechnik umstellen und vermehrt unbestimmte Rechtsbegriffe und vollständig technikneutrale Formulierungen wählen. Schutzobjekt der Vorschriften ist die im elektronischen Rechnungsbeleg verkörperte Willenserklärung **gegenüber dem Fiskus**.<sup>46</sup> Welches Verfahren man auch immer ersinnen will, um es unter die Norm zu subsumieren, es muss diesem Schutzziel gerecht werden können. Das bedeutet freilich nicht, dass es dazu perfekter Sicherheit bedarf, die es ohnehin nicht gibt. Die Frage der Bewertung, ob ein Verfahren ein angemessenes Sicherheitsniveau i. S. d. Vorschriften erreicht, ist also noch nicht entschieden und wird nachfolgend noch zu beleuchten sein.

## V. Der Rechnungsbegriff und die drei Sicherheitsziele

### 1. Der neue Rechnungsbegriff nach Art. 217

Art. 217 lautet: „Im Sinne dieser Richtlinie bezeichnet der Ausdruck ‚elektronische Rechnung‘ eine Rechnung, welche die nach dieser Richtlinie erforderlichen Angaben enthält und in einem elektronischen Format ausgestellt und empfangen wird.“<sup>47</sup>

Im Vergleich zur alten Regelung fällt lediglich auf, dass der Richtliniengeber die Begriffspaare „Übermittlung oder Bereitstellung“ in der neuen Fassung auf „ausgestellt und empfangen“ geändert hat. Damit wird deutlicher formuliert, dass auch im elektronischen Geschäftsverkehr die „**Begebung**“<sup>48</sup> der Rechnung ein zwingendes Tatbestandsmerkmal ist. Auch auf Online- und Konsolidierungsplattformen ist ein Sphärenwechsel des elektronischen Belegs vom Aussteller zum Empfänger erforderlich, den der Aussteller der Rechnung oder Gutschrift initiieren muss. Allein die Möglichkeit des Leistungsempfängers, eine Rechnung im System des Ausstellers abrufen zu können, genügt nicht, um den Anspruch des Leistungsempfängers (§ 14 Abs. 2 UStG) auf Ausstellung einer Rechnung zum Erlöschen zu bringen.<sup>49</sup>

## 2. Die drei übergreifenden Sicherheitsziele

Der Richtliniengeber formuliert nun vorab in Art. 233 insgesamt **drei zentrale Sicherheitsziele** und gibt nachfolgend geeignete Verfahren an. Hierbei unterscheidet er **organisatorische Verfahren** und **technische Verfahren**. Die Aufzählung ist jedoch nicht abschließend.<sup>50</sup> Die drei zentralen Sicherheitsziele formuliert der Richtliniengeber wie folgt:

Art. 233 Abs. 1 Satz 1: „Die **Echtheit der Herkunft** einer Rechnung, **die Unversehrtheit ihres Inhalts** und **ihre Lesbarkeit** müssen unabhängig davon, ob sie auf Papier oder elektronisch vorliegt, **vom Zeitpunkt der Ausstellung bis zum Ende der Dauer der Aufbewahrung** der Rechnung **gewährleistet** werden.“

Die systematische Umstellung, allgemeine Sicherheitsziele vor die Klammer zu ziehen, war erforderlich geworden, um dem Wunsch einer Liberalisierung der Sicherheitsvorschriften und einer stärker technikneutralen Formulierung nachkommen zu können. Das Voranstellen allgemeiner und gesetzlich definierter Sicherheitsziele für E-Rechnungen war ursprünglich nicht im Entwurf der EU-Kommission für die Richtlinie 45/2010 enthalten.<sup>51</sup> Die nun erfolgte Aufnahme ist das Ergebnis des Konsultationsverfahrens, in dem eine Vielzahl von Experten eine solche allgemeine Fixierung von Sicherheitszielen verlangt hatte, um andere und insbesondere von der Richtlinie nicht näher bestimmte Verfahren sinnvoll beurteilen zu können.<sup>52</sup>

Im Einzelnen:

#### a) „Echtheit der Herkunft“ (Authentizität)

Nach Art. 233 Abs. 1 Satz 4: „bedeutet Echtheit der Herkunft **die Sicherheit der Identität** des Lieferers oder des Dienstleistungserbringers oder **des Ausstellers** der Rechnung.“

44 Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW), 12 900 Mitglieder umfassender Berufsverband der Wirtschaftsprüfer in Deutschland.

45 Information Systems Audit and Control Association (ISACA), Weltverband der IT-Revisoren mit mehr als 86 000 Mitgliedern aus über 160 Ländern.

46 Nach der h. M. enthält die elektronische Rechnung ein Anerkenntnis der Umsatzsteuerschuld gegenüber dem Fiskus; vgl. dazu *Rossmagel*, Fremdsignierung elektronischer Rechnungen: Vorsteuerabzug gefährdet, BB 2007 S. 1234; so auch *Kirmes*, Forum elektronische Steuerprüfung 6/2006; *Kirmes*, eBilling im Intermediärmodell: Der Versand elektronischer Rechnungen (§ 14 Abs. 3 UStG) über Dienstleister – ein Problem des Mehrvertretungsverbots (§ 181 BGB), StB 2009 S. 75, 77, Fn. 31.

47 RL 2010/45/EU des Rates vom 13. 7. 2010.

48 *Wagner* in Sölch/Ringleb, § 14c Rz. 181, mit Hinweis auf § 13 Abs. 1 Nr. 4 UStG.

49 Vgl. zu dieser Problematik ausführlich *Kirmes*, eBilling im Intermediärmodell: Der Versand elektronischer Rechnungen (§ 14 Abs. 3 UStG) über Dienstleister – ein Problem des Mehrvertretungsverbots (§ 181 BGB), Steuerberater 3/2009 S. 80, m. w. N.

50 Wortlaut Art. 233 Abs. 2: „lassen sich die folgenden Beispiele von Technologien anführen“.

51 Im Entwurf der Kommission war lediglich die vollständige Streichung der Art. 233, 234, 235 und 237 vorgesehen, vgl. KOM (2009) 0021 – C6–0078/2009 – 2009/0009 (CNS), S. 22.

52 Vgl. *Kirmes/Gass*, Stellungnahme an die Europäische Kommission des Software Industrieverbandes elektronischer Rechtsverkehr (SIV-ERV) zum Bericht KOM (2009) 21, Version: 1.5 vom Januar 2010, www.siv.erv.de., S. 14, Erläuterung zu Tz. 1.

Diese klarstellende Definition war lange überfällig und ebenfalls eine erfüllte Forderung aus der geäußerten Kritik im Konsultationsverfahren.<sup>53</sup> Die Authentizität einer elektronischen Transaktion kann nur technisch richtig konstruiert werden, wenn diese sich auf einen anerkannten oder vereinbarten Vertrauensanker bezieht. Dieser Vertrauensanker ist nun de lege lata definiert als **sichere Identität**.<sup>54</sup> Der deutsche Gesetzgeber ergänzt in der Gesetzesbegründung für die Umsetzung in das nationale Recht: „Unter Echtheit der Herkunft ist die Sicherheit der Identität des Rechnungsausstellers (leistender Unternehmer oder Leistungsempfänger in dem Fall der Gutschrift oder Dritter, sofern sich der leistende Unternehmer oder der Leistungsempfänger in dem Fall der Gutschrift eines Dritten zur Rechnungsstellung bedient) zu verstehen“.<sup>55</sup>

Die Regelung muss im Zusammenhang mit dem Vorsteuerabzug gesehen werden. Es ist durch den Aussteller der Rechnung zu klären, wie es dem Rechnungsempfänger durch ein vom Aussteller gewähltes System ermöglicht wird, die im Rechnungsbeleg angegebene (behauptete) Identität zu überprüfen (Verifikation). Das heißt, die Angaben im Beleg (nach Art. 226, **Name und vollständige Anschrift**)<sup>56</sup> müssen sicher übertragen werden und für den Empfänger und den Fiskus verifizierbar sein. Das wird in Geschäftsbeziehungen, denen eine längere Vertragsverhandlung und eine Bonitätsprüfung vorausgehen, unproblematisch der Fall sein.<sup>57</sup> In all jenen Fällen jedoch, in denen der Vertrag ad hoc und weitgehend anonymisiert (also insbesondere im Internet) zustande kommt, stellt sich das Problem der Verifizierbarkeit „sicherer Identitäten“ in seiner ganzen Breite. Notwendig sind dann Systeme, deren technische Authentifizierungsinfrastruktur eine sichere Identifizierung der Teilnehmer an diesem System absichert. Wie bisher kann die Authentifizierungsfunktion der qualifizierten E-Signatur gem. Art. 233 Abs. 2 Buchst. a) genutzt werden.<sup>58</sup> Daneben können nun aber auch alternative Verfahren eingesetzt werden. Hier sind insbesondere der elektronische Identitätsnachweis des neuen Personalausweises gem. § 18 Abs. 1 PAuswG<sup>59</sup> und der Versanddienst gem. § 3 i. V. m. § 5 De-Mail-Gesetz<sup>60</sup> zu nennen. Auch denkbar ist die Nutzung der elektronischen Abfragemöglichkeiten zur Umsatzsteueridentifikationsnummer, sofern der Aussteller über eine solche verfügt und diese im Beleg angibt.<sup>61</sup> In Einzelfällen denkbar erscheint auch eine sog. Fernidentifizierung über die Kontoverbindung i. S. d. Geldtransferverordnung.<sup>62</sup> Jedenfalls beschreibt das BMF ein solches Verfahren in seinen FAQ.<sup>63</sup> Allerdings dürfte das praktische Einsatzfeld dieses Verfahrens sehr begrenzt sein.<sup>64</sup>

**b) „Unversehrtheit des Inhalts“ (Integrität)**

Nach Art. 233 Abs. 1 Satz 5 bedeutet: „Unversehrtheit des Inhalts“, dass der nach der vorliegenden Richtlinie erforderliche Inhalt nicht geändert wurde“.<sup>65</sup>

Ohne Unterschiede insoweit auch der deutsche Gesetzgeber:

„Unversehrtheit des Inhalts liegt vor, wenn die nach dem Umsatzsteuergesetz erforderlichen Angaben nicht geändert wurden.“<sup>66</sup>

Der Integritätsschutz in den („klassischen“) Verfahren nach Art. 233 Abs. 2 Buchst. a) und b) (Signatur und EDI) wird über kryptographische Verfahren sichergestellt.<sup>67</sup> Fraglich ist, wie die Anforderung des Integritätsschutzes von organisatorischen Verfahren (verlässlicher Prüfpfad) erreicht werden kann. Nun ist derlei nicht schlichtweg unmöglich. Ganz im Gegenteil gibt es eine Vielzahl von IT-Sicherheitsmodellen, die Integritätsschutz als zentrale Aufgabe definieren.<sup>68</sup> Die Durchsetzbarkeit solcher Verfahren hängt jedoch davon ab, ob ihre Regeln mittels ei-

53 *Kirmes/Gass*, Stellungnahme an die Europäische Kommission des Software-Industrieverbandes elektronischer Rechtsverkehr (SIV-ERV) zum Bericht KOM (2009) 21, Version: 1.5 vom Januar 2010, www.siv.erv.de, S. 14, Erläuterung zu Tz. 5.  
 54 Nun nicht mehr haltbar die Auffassung von *Groß/Lindgens*, UVR 2008 S. 113, Nr. 2 „die elektronische Rechnung erfordere keine Identifikationsfunktion“; vgl. zur Kritik bereits *Kirmes*, StB 2009 S. 75, 77, Fn. 18.  
 55 Vgl. Gesetzesbegründung zum StVereinfG 2011, BT-Drucks. 17/5125 S. 75.  
 56 Auch gem. Art. 226b RL 112/2006 EG wird im Zusammenhang mit vereinfachten Rechnungen gem. Art. 220a und Art. 221 Abs. 1 und 2 nur „die Identität des Stpfl., der die Gegenstände liefert oder die Dienstleistungen erbringt“, verlangt.  
 57 Im Handelsverkehr wird Anonymität normalerweise nicht akzeptiert. Es liegen regelmäßig Verträge, Registerauszüge etc. vor, die den Vertragspartner sicher identifizieren (zumeist Urkundenbeweise). Diese Ermittlung ist auch nicht zusätzlich erforderlich, weil es im Interesse jedes Kaufmanns steht, den Vertragspartner mindestens insoweit zu identifizieren, dass eine wirksame Klage (Angaben im Rubrum, § 253 ZPO) eingereicht werden könnte (Obliegenheit).  
 58 Gem. § 14 Abs. 2 Signaturgesetz vom 16. 5. 2001, BGBl. I 2001 S. 876, zuletzt geändert durch Art. 4 des Gesetzes vom 17. 7. 2009, BGBl. I 2009 S. 2091, i. V. m. § 3 Abs. 1 Signaturverordnung vom 16. 11. 2001, BGBl. I 2001 S. 3074, zuletzt geändert durch Art. 1 der Verordnung vom 15. 11. 2010, BGBl. I 2010 S. 1542.  
 59 Personalausweisgesetz vom 18. 6. 2009, BGBl. I 2009 S. 1346.  
 60 Vgl. § 3 i. V. m. § 5 DMDG Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften, BT-Drucks. 17/3636 vom 8. 11. 2010.  
 61 Abfrageverfahren zur Umsatzsteueridentifikationsnummer, vgl. MwSt-Informationsaustauschsystem (MIAS), [http://ec.europa.eu/taxation\\_customs/vies/vieshome.do](http://ec.europa.eu/taxation_customs/vies/vieshome.do), (Stand 15. 2. 2011); das Bundeszentralamt für Steuern bietet eine Portal- und Webservice-Lösung zur Abfrage an, <http://evatr.bff-online.de/eVatR/xmlrpc/>.  
 62 Geldtransfer-Verordnung, EG 1781–2006.  
 63 Vgl. dort Fn. 14, letzter Anstrich S. 4.  
 64 Von einer Fernidentifizierung (geregelt in § 6 Abs. 3 GWG) spricht man in den Fällen, in denen der Vertragspartner von keiner natürlichen Person direkt identifiziert wird (non-face-to-face). Damit fällt das Post-Ident-Verfahren nicht unter die Fälle der Fernidentifizierung, da hier ein Mitarbeiter der Deutschen Post AG die Identifizierung vornimmt. Soweit ein Fall einer Fernidentifizierung vorliegt, müssen zwei Bedingungen erfüllt werden: Zum einen muss eine Kopie des Original-Lichtbildausweises zur Identifizierung vorliegen. Daneben muss zwingend die erste Transaktion von einem Konto des Vertragspartners erfolgen (z. B. Überweisung von 10 Cent). Damit soll verhindert werden, dass mit einem abhanden gekommenen Ausweis über die Identität getäuscht wird. Ebenfalls ausgeschlossen in diesem Verfahren sind jegliche Bartransaktionen; vgl. *Achtelik* in Herzog, GWG-Kommentar, 2010, S. 313 ff.  
 65 Art. 233 Satz 4 RL 112/2006 EG.  
 66 Vgl. Gesetzesbegründung zum StVereinfG 2011, BT-Drucks. 17/5125 S. 75.  
 67 Der Integritätsschutz wird sowohl bei der Signatur als auch beim EDI über Prüfsummen (Hashwerte) auf das transportierte Datenobjekt „Rechnung“ (= Datei) abgebildet.  
 68 Vgl. z. B. das „Biba-Modell“, *Biba*, „Integrity Considerations for Secure Computer Systems“, MTR-3153, Mitre Corporation, April 1977; das Biba-Modell ist eine Umkehrung des Bell-La Padula-Sicherheitsmodells, das Vertraulichkeit adressiert, vgl. *Bell/LaPadula*: Secure Computer Systems: Mathematical Foundations. MITRE Corporation, 1973; ebenfalls die Integrität schützt das „Clark Wilson-Modell“, vgl. *Clark/Wilson*, A Comparison of Commercial and Military Computer Security Policies. IEEE Symposium on Security and Privacy, 1987, S. 184.

nes sog. Referenzmonitors<sup>69</sup> implementiert werden können, was in heterogenen Infrastrukturen wie dem Internet alles andere als eine Kleinigkeit ist. Hier kann dem Stpfl. nur geraten werden, sich die Behauptungen von Herstellern oder Anbietern von entsprechenden Systemen<sup>70</sup> – diese verfügen über einen solchen „organisatorischen Integritätsschutz“ – jeweils durch Zertifikate<sup>71</sup> belegen zu lassen.<sup>72</sup>

**c) „Lesbarkeit“**

Völlig neu eingeführt durch die Richtlinie 45/2010 wurde das Tatbestandsmerkmal der „Lesbarkeit“. Unverständlich ist allerdings, warum die Richtlinie im Unterschied zu den anderen Tatbestandsmerkmalen hier **keine** Legaldefinition vornimmt. Mangels einer autonomen Definition in der Richtlinie ist der technikkrechtliche Begriff „Lesbarkeit“ primär anhand von europäischen technischen Normen zu definieren.<sup>73</sup> Einschlägig sind z. B. die ISO/IEC 19005–1<sup>74</sup> und der Standard UN/CEFACT – Cross Industry Invoice – V2<sup>75</sup> auf Grundlage der ISO-20022.<sup>76</sup> Aber auch ein Blick in das nationale Recht hilft bei der Eingrenzung der Anforderung. Nach § 257 Abs. 3 Nr. 2 HGB bedeutet „Lesbarkeit“, dass die empfangenen Handelsbriefe und Buchungsbelege „während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können“.

Es gilt insoweit, für die Lesbarkeit zwei Aspekte zu berücksichtigen. Die Lesbarkeit muss technisch dauerhaft möglich sein (**Formatproblem**) und in angemessener Zeit erfolgen können (**Zeitproblem**). Beim Zeitproblem ist zu beachten, dass das Steuerrecht über die handelsrechtlichen Pflichten hinausgeht, wenn es in § 147 Abs. 5 AO die „**unverzügliche**“ Lesbarmachung anstelle der in § 257 Abs. 3 Nr. 2 HGB geforderten „**angemessenen Frist**“ fordert.<sup>77</sup>

Das Formatproblem adressiert die Schwierigkeit, dass die identische Darstellung der archivierten Inhalte hardware-, software- und versionsunabhängig bei proprietären Datei-Formaten kaum über den notwendigen Prognosezeitraum von sechs bis zehn Jahren erbracht werden kann.<sup>78</sup> Das Vorhalten von Altsystemen (zur Darstellung) ist zudem teuer und nicht in jedem Fall ausreichend, weil der Fiskus verlangen kann, „ohne Hilfsmittel lesbare Reproduktionen beizubringen“ (§ 147 Abs. 5 AO).

Zudem muss das Formatproblem aus einer **zweiseitigen Perspektive** betrachtet werden. Die Aufbewahrungspflicht trifft Aussteller und Empfänger von Rechnungen gleichermaßen, so dass entweder Vereinbarungen über das Rechnungsformat getroffen werden müssen oder auf einen de-facto-Standard zurückgegriffen werden muss. Als de-facto-Standard wäre das europäisch und international normierte PDF/A-Format nutzbar. Auch im EDI-Verfahren wäre es zu bevorzugen, einen (zusätzlichen) monatlichen Sammelbeleg im Format PDF/A<sup>79</sup> zu erstellen und die Aufbewahrungspflichten damit auf diesen Sammelbeleg zu reduzieren, anstatt alle XML- oder EDIFACT-

Dateien der Aufbewahrung und damit auch dem Problem der Lesbarkeit zu unterwerfen.

**VI. Die „klassischen“ technischen Systeme**

Die Streichung der Abweichungsbefugnisse in Art. 233 Abs. 2 Richtlinie 112/2006 EG a. F., die Neufassung des Art. 233 Abs. 2 und die Streichung von Art. 233 Abs. 1 Unterabs. 1, Art. 233 Abs. 3 und Art. 234 Richtlinie 112/2006 EG a. F. verbessert die europaweite Nutzbarkeit von EDI und Signaturlösungen nachhaltig. In Art. 233 Abs. 2 heißt es nun: „Neben der in Absatz 1 beschriebenen Art von innerbetrieblichen Steuerungsverfahren lassen sich die folgenden Beispiele von Technologien anführen (...)

**a) durch eine fortgeschrittene elektronische Signatur (...), die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit (...)** erstellt worden ist; **b) durch elektronischen Datenaustausch (EDI) (...), sofern in der Vereinbarung über diesen Datenaustausch der Einsatz von Verfahren vorgesehen ist, die die Echtheit der Herkunft und die Unversehrtheit der Daten gewährleisten.“**

Damit wurden **alle nationalen Abweichungsbefugnisse**, die in der Praxis zu erheblichen Interoperabilitätsproblemen führten, **vollständig beseitigt**.

69 Ein Referenzmonitor ist eine logische Einheit, die für die Kontrolle und Durchsetzung von Zugriffsrechten oder Dateizuständen zuständig ist. Das heißt, der Referenzmonitor entscheidet anhand einer Regelsammlung für jeden Zugriff eines Subjekts (also eines Akteurs wie Benutzers oder Prozesses) auf ein Objekt (Daten beliebiger Art) anhand von Regeln, ob der Zugriff erlaubt wird oder nicht; vgl. zum Begriff: *Eckert, IT-Sicherheit*, 6. Aufl. 2009, S. 574.

70 Denkbar ist hier wieder jedes System für Buchhaltung, Dokumentenmanagement, Archiv oder Onlinesystem, jedoch verfügen in der Praxis nur die wenigsten Systeme tatsächlich über solche Nachweise. Die schlichte Zusage des Herstellers erfüllt jedoch kaum die Sorgfaltsverpflichtungen einer geeigneten Systemauswahl.

71 Z. B. Common Criteria/ISO/IEC 15408, IDW-PS 880, 951.

72 Wird dagegen doch in der Implementierung auf kryptographische Verfahren zurückgegriffen, sind die Maßstäbe der qualifizierten elektronischen Signatur mindestens im Hinblick auf die Algorithmenauswahl anzusetzen; zu beachten sind die amtlichen Veröffentlichungen der Bundesnetzagentur, „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“, veröffentlicht z. B. am 1. 2. 2011 im Bundesanzeiger Nr. 17 S. 383.

73 Der Vorrang europäischer technischer Normen vor nationalen Regelungen ergibt sich aus dem Zusammenspiel des Vorrangs von supranationalen Rechtsakten (einschl. der Verweise) und dem sog. „New and Global Approach“ für technische Normung in der EU; vgl. „Entschließung des Rates zu einem Gesamtkonzept für die Konformitätsbewertung“, ABl. Nr. C 10 vom 16. 1. 1990, und „Beschluss des Rates über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren“, ABl. Nr. L 380 vom 31. 12. 1990; vgl. zur aktuellen Rechtslage in Deutschland *Gesmann-Nuissl, Ensthaler, Edelhäuser, KAN-Bericht 47*, www.kan.de.

74 ISO/IEC 19005–1, Document Management – Electronic document file format for long term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).

75 Entwurf des UN/CEFACT, Cross Industry Invoice v2 (Requirements Specification Mapping Cross Industry Invoicing Process) vom 3. 7. 2009, Version 2.00.08, abrufbar unter: www.unece.org.

76 ISO 20022 Financial Services – Universal financial industry message scheme.

77 Umsatzsteuer Anwendungserlass (UStAE) vom 1. 10. 2010, IV D 3 – S 7015/10/10002, 2010/0815152.

78 Vgl. *Oettler/Drümmer/von Seggern*, PDF/A kompakt, Digitale Langzeitarchivierung mit PDF, Callas Software GmbH, 2007; *Zellmann*, Documanager 9/2005, Der neue ISO-Standard PDF/A zur Langzeitarchivierung: Weshalb, wie und für wen?, www.documanager.de.

79 Ggf. mit Absicherung durch eine qualifizierte E-Signatur.

Es entbehrt nicht einer gewissen Ironie, dass die beiden „klassischen“ Verfahren EDI und qualifizierte E-Signatur, die im Konsultationsverfahren erheblicher Kritik unterlagen, am Ende so deutlich gestärkt aus dem Gesetzgebungsverfahren hervorgehen. Wie sich noch zeigen wird, sind im Ergebnis beide Verfahren derzeit die sichersten und am einfachsten einzusetzenden Verfahren zur Nutzung der elektronischen Rechnung.

## VII. Organisatorische Sicherheitsmaßnahmen

### 1. Charakterisierung des Prüfpfades

Wenden wir uns nun dem wohl interessantesten Teil der Richtlinie zu, den neuen organisatorischen Sicherungsverfahren durch „verlässlichen Prüfpfad“.

Art. 233 Abs. 1 Satz 3 formuliert: „Dies (die drei Sicherheitsziele)<sup>80</sup> können durch jegliche **innerbetriebliche Steuerungsverfahren** erreicht werden, die einen **verlässlichen Prüfpfad** zwischen **einer Rechnung** und **einer Lieferung oder Dienstleistung** schaffen können“.<sup>81</sup>

Der deutsche Gesetzgeber formuliert in § 14 Abs. 1 Satz 3 UStG n.F. „Dies kann durch jegliche innerbetriebliche **Kontrollverfahren** erreicht werden, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können.“<sup>82</sup>

Auch hier verzichtet der Richtliniengeber auf eine Legaldefinition. Die Formulierung „Prüfpfad“ ist allerdings ein bekannter Terminus<sup>83</sup> aus dem europäischen Zollrecht (gewissermaßen ein „naher Verwandter“ des europäischen Umsatzsteuerrechts). Die Eigentümlichkeit des Begriffs und der Verzicht auf eine richtlinienautonome Legaldefinition lassen den Schluss zu, dass offenbar bewusst auf den etablierten Begriff „Prüfpfad“ des europäischen Zollrechts abgestellt werden soll.<sup>84</sup>

Auch teleologisch spricht die nahezu kongruente Problemstellung für eine Übernahmeabsicht, denn auch im europäischen Zollkodex geht es um die Definition von organisatorischen Anforderungen, die Vertrauen der Behörden in die innerbetrieblichen Abläufe der Unternehmen etablieren sollen.<sup>85</sup>

Nach den Zoll-Leitlinien der Europäischen Kommission wird unter einem „Prüfpfad“ ein **Verfahren** verstanden, „mit dem man **jede Eintragung in der Buchhaltung** bis zu **ihrer Quelle zurückverfolgen** kann, um deren Richtigkeit zu prüfen. Ein vollständiger Prüfpfad ermöglicht es, den **Lebenszyklus betrieblicher Vorgänge** zu verfolgen, d. h. in diesem Zusammenhang **den Fluss von Waren und Produkten, die in das Unternehmen eingehen, verarbeitet werden und das Unternehmen wieder verlassen**. Viele Unternehmen und Organisationen haben aus Sicherheitsgründen einen solchen Prüfpfad in ihren automatisierten Systemen. Über den Prüfpfad wird der **Weg der Daten im zeitlichen Ablauf**

**erfasst**; auf diese Weise kann jeder Datensatz vom Augenblick des Eingangs in die Buchführung des Unternehmens bis zur Ausbuchung verfolgt werden.“<sup>86</sup>

Auch die Anforderungen an ein geeignetes System der Buchführung werden unter dem Stichwort „**Zufrieden stellendes System der Buchführung**“ in Art. 5a Abs. 2 Unterabs. 1 Anstrich 2 ZK i. V. m. Art. 14i ZKDVO konkretisiert. „Die Buchführung muss den **Erfordernissen des nationalen Rechts entsprechen**, (...) zur **Erkennung illegaler oder nicht ordnungsgemäßer Vorgänge geeignet** sein (...), Schutz **vor Informationsverlust** bieten (...) und in **geeigneter Weise gegen unbefugtes Eindringen** gesichert sein.“<sup>87</sup> Nach Art. 14i Unterabs. 1 Buchst. a–f ZKDVO kann der Nachweis der Eignung erbracht werden über Prüfberichte von Wirtschaftsprüfern oder durch Zertifikate<sup>88</sup> zur GoBS<sup>89</sup>-Konformität.<sup>90</sup>

Legt man den Maßstab der zollrechtlichen Definition zu Grunde, setzt sich ein „verlässlicher Prüfpfad“ als organisatorisches Verfahren aus insgesamt vier kumulativ zu erfüllenden Komponenten zusammen:

- 1) ein „**zufrieden stellendes System der Buchführung**“,

80 Die Klammereinfügung erfolgte durch den Verfasser.  
 81 Einführung zur RL 2010/45/EU des Rates vom 13. 7. 2010, Nr. 10.  
 82 Völlig falsch die Begründung im Referentenentwurf zum Steuervereinfachungsgesetz 2011 vom 20. 12. 2010, S. 75, 3. Abs.: „Art. 233 Absatz 1 Satz 2 Mehrwertsteuer-Systemrichtlinie räumt den Mitgliedstaaten jedoch ebenfalls die Möglichkeit ein, auch andere elektronische Rechnungen anzuerkennen. Von dieser Option wird nunmehr Gebrauch gemacht.“ Das ist Unsinn, denn die Abweichungsbefugnisse wurden gerade mit der Änderungsrichtlinie 45/2010 EU gestrichen. Die neuen Regelungen sind zwingend von allen Staaten umzusetzen und gerade nicht die Folge nationaler Abweichungsbefugnisse, die wieder auf eine inhereuropäische Inkompatibilität hinauslaufen würden.  
 83 Eine sprachliche Analyse und ein Vergleich mit den gem. Art. 55 EU-Vertrag gleichermaßen geltenden anderen Sprachfassungen legte schließlich die Spur zum „großen Unbekannten“; EN: „This may be achieved by any business controls which create a reliable audit trail between an invoice and a supply of goods or services“; FR: „Cela peut être réalisé par des contrôles de gestion qui établiraient une piste d'audit fiable entre une facture et une livraison de biens ou de services.“; PL: „Można to zapewnić za pomocą dowolnych kontroli biznesowych, które ustalają wiarygodną ścieżkę audytu między fakturą a dostawą towarów lub świadczeniem usług.“  
 84 Vgl. *Riesenhuber*, Europäische Methodenlehre, 2010, § 11 Die Auslegung, S. 315 ff.  
 85 Vgl. *Witte*, Zollkodex mit Durchführungsverordnung und Zollbefreiungsverordnung, Kommentar, 4. Aufl., S. 97 ff.  
 86 EU-Kom; TAXUD/2006/1450; zugelassene Wirtschaftsbeteiligte (Authorized Economic Operators – AEO), Leitlinien zu Standards und Kriterien vom 29. 6. 2007, Unterabschn. 3.01 „Prüfpfad“.  
 87 *Harings* in Dorsch, Zollrecht, Art. 5a ZK, Rz. 73 ff., mit Verweis auf *Wolffgang/Natzel*, ZfZ 2006 S. 357; *Rüsken* (Hrsg.), Zollkodex und Durchführungsverordnungen, 3. Aufl., Oktober 2010; BMF vom 7. 11. 1995, IV A 8 – S 0316 – 52/95 (GoBS), BStBl 1995 S. 738, BMF, AEO-DV Rz. 242, Kommission, Leitlinien, S. 11; vgl. auch ohne Abweichung Zollglossar von *Witte* in Lehrbuch des Europäischen Zollrechts von *Witte/Wolfgang*, 5. Aufl.; *Witte*, Zollkodex mit Durchführungsverordnung und Zollbefreiungsverordnung, 4. Aufl.  
 88 IDW-PS 880, IDW Prüfungsstandard: „Die Prüfung von Softwareprodukten“, Stand: 11. 3. 2010; ebenfalls geeignet sind Zertifikate nach IDW PS 951, IDW Prüfungsstandard: „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“, Stand: 9. 9. 2010; Zertifikate auf Basis der ISO/IEC 15408 ff.  
 89 BMF vom 7. 11. 1995, IV A 8 – S 0316 – 52/95 (GoBS), BStBl 1995 S. 738.  
 90 BMF, AEO-DV Rz. 242.

- 2) eine **lückenlose Lieferkettenerfassung** (supply chain-Managementsystem),
- 3) die auf einer **Papierspur (Verträge/Identifizierungen)** aufsetzt und
- 4) in einer **sicheren IT-Umgebung** betrieben wird.

Es geht mithin um eine **mittelbare Zuordnung** der Identität des Ausstellers/Leistenden über die Lieferkette (supply chain) durch:

- 1) eine Zuordnung von Belegen/Transaktionen zur Dienstleistung oder Ware
- 2) und dann **mittelbar** über die Vertragskette (Papierspur) zum Aussteller der Rechnung.

Der verlässliche Prüfpfad kann im Ergebnis die Identität eines Rechnungsausstellers verifizieren und auch „Scheinleistungen“ in Betrugskonstellationen wirksam bekämpfen.

Um für die Praxis konkrete Umsetzungshinweise zu erhalten, ist die Lektüre der „Leitlinien zu Standards und Kriterien für Authorized Economic Operators – AEO“,<sup>91</sup> die eine umfangreiche tabellarische Systematik von Anforderungen und konkreten Handlungsempfehlungen für die Unternehmen aussprechen, empfohlen.

Wichtig erscheint noch der Hinweis, dass der verlässliche Prüfpfad als Verfahrensoberbegriff für verschiedene ganz unterschiedliche Maßnahmen kein „Allheilmittel“ ist. Wie jedes andere Verfahren ist jeweils zu prüfen, welches der drei Sicherheitsziele im konkreten Einsatzumfeld wirksam abgedeckt werden kann (dazu sogleich vertieft).

**Zwischenergebnis:**

Bis hierher kann man zusammenfassen, dass es drei zentrale Sicherheitsziele gibt, die jeweils durch technische oder organisatorische Verfahren (für einen verlässlichen Prüfpfad) abgesichert werden können. Der Rechnungsaussteller hat die Wahl und trägt das Auswahlrisiko eigenverantwortlich.

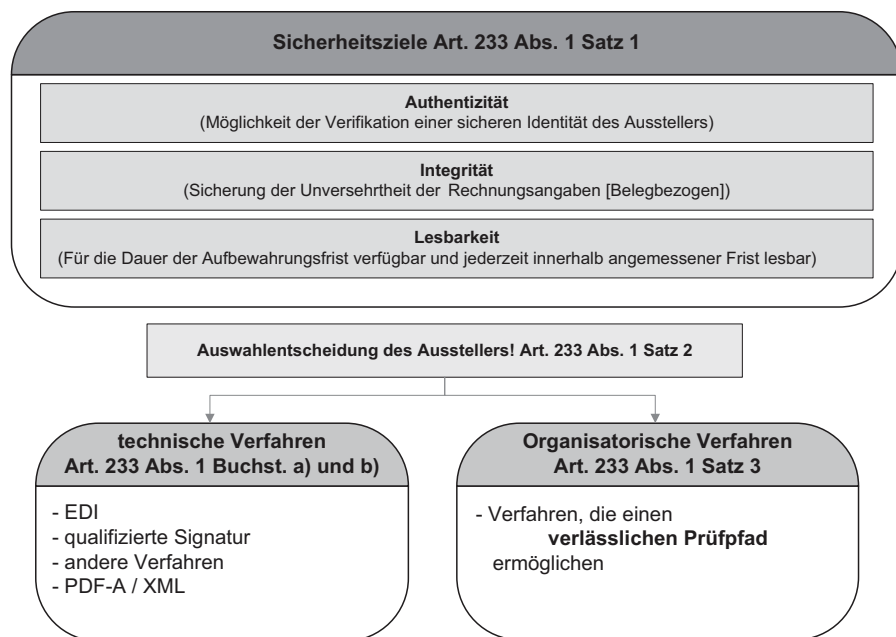


Abb. 1: Zusammenfassung Regelungsstruktur E-Rechnung



Abb. 2: Risikopfade nach Art der Geschäftsverbindung

**2. Risikoorientierte Unterscheidung nach Art der Geschäftsverbindung**

Um nun in der Praxis vom abstrakten Lösungsppluralismus zu einer konkreten Anwendung im Unternehmen zu gelangen, schlage ich vor, grundsätzlich zwei Einsatzfelder zu unterscheiden: **(1)** die „**ständige Geschäftsverbindung**“ und **(2)** die „**Ad-hoc-Geschäftsverbindung**“.

Eine **ständige Geschäftsverbindung (1)** zeichnet sich dadurch aus, dass sich die Geschäftspartner vor Durchführung eines Leistungsaustauschs kennen. Eine Identifizierung i. S. d. § 4 GwG wird dabei in den seltensten Fällen stattgefunden haben. Aber Kaufleute pflegen z. B. die Vertretungsmacht des Verhandlungspartners über Handelsregisterdaten und die wirtschaftliche Lage anhand

<sup>91</sup> EU-Kom; TAXUD/2006/1450; zugelassene Wirtschaftsbeteiligte (Authorized Economic Operators – AEO), Leitlinien zu Standards und Kriterien vom 29. 6. 2007.

von Wirtschaftsauskünften oder über das amtliche Unternehmensregister zu überprüfen. In diesen Fällen entsteht auf Grund der Vorverhandlungen auf **beiden Seiten** des Leistungsaustauschs eine Papierspur, die regelmäßig keinen Zweifel an der Identität der Vertragspartner aufkommen lässt.<sup>92</sup>

Im Gegensatz dazu ist die **Ad-hoc-Geschäftsverbindung (2)** dadurch gekennzeichnet, dass der Leistungsaustausch oder mindestens die Verpflichtung zu einem solchen ohne vorherige (genaue oder valide) Kenntnis der Identität des Kontrahenten erfolgt und die Anbahnung über eine Distanz (also im Internet oder per Telefon) stattfindet. Als Beispiel wäre ein Online-Shop, der im B2B-Bereich tätig ist, exemplarisch.<sup>93</sup>

Im Kern geht es bei der Unterscheidung darum, einen risikoorientierten Ansatz für die Auswahl und Kombination geeigneter Verfahren anzuwenden. Die Differenzierung ist sinnvoll, weil in ständigen Geschäftsverbindungen bei geringerem Risiko<sup>94</sup> und auf Grund der engeren Verbindung und der Möglichkeit, zweiseitige Vereinbarungen auszuhandeln (z. B. über die auf beiden Seiten dauerhaft lesbaren Formate und gesicherte Transport-Kanäle), in deutlich größerem Umfang organisatorische Verfahren für einen verlässlichen Prüfpfad eingesetzt werden können.

ziele zusammenwirken müssen. Diese Notwendigkeit wird am besten am Beispiel der qualifizierten E-Signatur (QS) illustriert. Die QS ist bestens geeignet, die Sicherheitsziele Authentizität und Integrität zu gewährleisten. Jedoch ist das Verfahren hinsichtlich des Sicherheitsziels „Lesbarkeit“ schlicht ungeeignet. Erst die Kombination von verschiedenen Verfahren ermöglicht einen rechtskonformen elektronischen Rechnungsversand. Im Beispiel wäre also die Erstellung einer Rechnung als qualifiziert signiertes PDF/A-Dokument eine uneingeschränkt für jeden Anwendungsfall geeignete Verfahrenskombination.

Es ist mithin **immer** erforderlich, **jedes** Verfahren (organisatorisch oder technisch) im konkreten Einsatzszenario auf Eignung für die drei Sicherheitsziele (Authentizität/Integrität/Lesbarkeit) zu hinterfragen. Aus der tabellari-schen Übersicht in Abbildung (4) wird deutlich, dass die Eignung der Verfahren je nach Geschäftsverbindungstyp variiert.

Weiterhin darf nicht aus dem Auge verloren werden, dass es sich beim elektronischen Rechnungsversand um ein „zweiseitiges Sicherheitsproblem“ handelt.<sup>95</sup> Das bedeutet, dass der Rechnungsaussteller entweder die Fähigkeiten und Möglichkeiten des Empfängers antizipiert oder mit dem Empfänger konkret aushandelt. Insbesondere bei der Nutzung von organisatorischen Verfahren, die

einen verlässlichen Prüfpfad ermöglichen, muss der Aussteller bei seiner Auswahl immer den Kunden (Rechnungsempfänger) in den Fokus seiner Überlegungen stellen.

Nur die Fähigkeiten oder Verfahren, die beim Empfänger (ebenfalls) vorliegen, ermöglichen die Sicherstellung der Sicherheitsziele. Kann der Aussteller/Leistende dagegen die Verfahren des Empfängers nicht einschätzen oder sind diese nicht vertrauenswürdig in Bezug auf die drei Sicherheitsziele, muss er auf ein Verfahren zurückgreifen, das

unabhängig von den Möglichkeiten beim Kunden/Empfänger die Sicherheit gewährleistet. Dieser Umstand wird durch die FAQ des BMF mindestens missverständ-

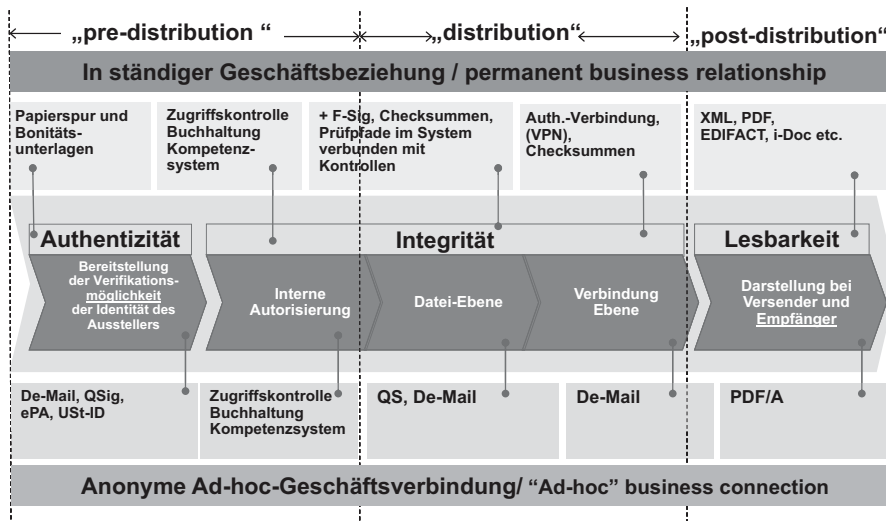


Abb. 3: Matrix Geschäftsart/Verfahren

Ein Unternehmen, das im Wesentlichen in ständigen Geschäftsverbindungen agiert, wird also deutlich mehr Gestaltungsmöglichkeiten entwickeln können als ein Unternehmen, das ständig wechselnde und neue Kundschaft im Internet adressiert.

### 3. Das Kombinationsproblem und die „zweiseitige Sicherheit“

Ein weiteres Problem in der praktischen Umsetzung liegt in dem Erfordernis zur Kombination der verschiedenen Verfahren, die kohärent in Bezug auf die drei Sicherheits-

92 Sind auf Grund der Rechtsform keinerlei registermäßige Recherchen möglich, sind bei Fernabwicklungen Ausweisdaten zu erfassen, will man den Prüfpfad nutzen. Allerdings genügt im Gegensatz dazu der gute alte „Handschlag“ bei persönlichen Treffen, da er die Anforderungen an eine face to face-Identifizierung erfüllt.

93 Vgl. z. B. [www.mercateo.com/](http://www.mercateo.com/).

94 Denn hier kann ein Know your customer (KYC)-Prinzip geltend gemacht werden.

95 Zum Problem der zweiseitigen Sicherheit grundlegend *Rannenber*, Kriterien und Zertifizierung mehrseitiger IT-Sicherheit, erschienen in *Ausgezeichnete Informatikdissertationen 1997*, Hrsg. Nominierungsausschuss des Dissertationspreises im Auftrag der Gesellschaft für Informatik (GI), 1998.

lich dargestellt. Dort wird suggeriert, der Aussteller würde eine „einsame“ Entscheidung treffen können, die sich nur nach den internen betrieblichen Abläufen ausrichtet.<sup>96</sup> Das Gegenteil ist der Fall. Wie schon immer liegen die Probleme bei der Nutzung elektronischer Rechnungen insbesondere darin, die Empfänger der Rechnungen sinnvoll in das System zu integrieren. Daran hat sich nichts geändert und auch der verlässliche Prüfpfad kann dieses grundsätzliche Systemdilemma nicht lösen oder mildern. Verfügt der Rechnungsempfänger z. B. nicht über eine verlässliche Buchführung (z. B. weil er nicht buchführungspflichtig ist) und kann er das EDIFACT-Format des Rechnungsausstellers weder anzeigen noch „lesbar“ aufbewahren, ist ein darauf basierendes Konzept des Ausstellers unbrauchbar.

hier soeben besprochenen Formvorschriften.<sup>98</sup> Diese Einschätzung trifft **nicht** zu, was durch den europäischen und deutschen Gesetzgeber im Rahmen der Gesetzesänderung nochmals bestätigt wurde.<sup>99</sup> Im Grundsatz gilt: Freiwilligkeit begründet keine Formerleichterung, § 146 Abs. 6 AO. Die Richtlinie 112/2006 EG nennt abschließend alle bestehenden Formerleichterungen. Eine Formerleichterung wegen Versand von Rechnungen „an private Rechnungsempfänger“ ist nicht existent.<sup>100</sup> In Art. 221 Abs. 3 wird den Mitgliedstaaten zwar eine Befugnis eingeräumt, die Stpfl. „von der Pflicht nach Art. 220 Abs. 1 (...), eine Rechnung auszustellen, (...) **mit oder ohne Recht auf Vorsteuerabzug** (...)“ zu befreien. Davon hat Deutschland bislang jedoch keinen Gebrauch gemacht.

Es bleibt deshalb bei dem gefestigten Grundsatz der AO. Möge man die „Ent-Bürokraten“ nach den Hintergründen befragen, warum hier eine mögliche Erleichterung ungenutzt geblieben ist.

## 2. Langzeitarchivierung von Signaturen bei E-Rechnung?

Ein erhebliches Problem ergibt sich aus der Änderung der europarechtlichen Vorgaben für

	permanent relationship			Ad-hoc connection		
<b>Authentizität</b>						
<b>Integrität</b>						
<b>Lesbarkeit</b>						
qualifizierte elektronische Signatur	n.a.	.+++	.+++	n.a.	.+++	.+++
electronic Data Interchange (EDI)	.++	.++	.	n.a.	n.a.	n.a.
De-Mail	n.a.	.+++	.+++	n.a.	.+++	.+++
neuer Personalausweis (ohne QS)	n.a.	n.a.	.+++	n.a.	n.a.	.+++
Ust-ID-Check	n.a.	n.a.	.	n.a.	n.a.	.
Prüfpfad (Audit-Trail)	n.a.	.	.++	n.a.	n.a.	n.a.
PDF/A	.+++	n.a.	n.a.	.+++	n.a.	n.a.
XML (XML-D-Sig) und EDIFACT etc.	.	.	n.a.	.	n.a.	n.a.
UN/CEFACT - Cross Industry Invoice - V2	.+++	.	n.a.	.++	n.a.	n.a.

n.a. = nicht anwendbar/ungeeignet  
 .+ = eingeschränkt geeignet bei zweiseitiger Vereinbarung

## Ende der Vorschau

### 1. Rechnungen in B2C-Verbindungen

Es hält sich hartnäckig das Gerücht, Rechnungen, die an eine Privatperson fakturiert werden, unterliegen nicht den

zur Diskussion über Formerleichterungen beim elektronischen Rechnungsversand an Private, [www.elektronische-steuerprüfung.de](http://www.elektronische-steuerprüfung.de).

100 Vgl. Art. 219a „Abweichend von Absatz 1 und unbeschadet des Art. 221 Absatz 2 ist die Ausstellung einer Rechnung bei nach Art. 135 Absatz 1 Buchstaben a bis g steuerbefreiten Dienstleistungen nicht erforderlich.“, d. h., bei Privatpersonen besteht keine Entlastung.

men.<sup>101</sup> Durch die Hinzufügung der Formulierung in Art. 233 Abs. 1 Satz 1 letzter Teil „bis zum Ende der Dauer der Aufbewahrung der Rechnung gewährleistet werden“, die auch vom deutschen Gesetzgeber in § 14b Abs. 1 Satz 2 UStG<sup>102</sup> übernommen wurde, bestehen ernstliche Zweifel, ob diese Praxis Bestand haben kann. Andernfalls wären nun auch elektronische Rechnungsdokumente einer **Signaturerneuerung**<sup>103</sup> zu unterziehen, was eine sehr teure Verschärfung der Aufbewahrungspflichten bedeuten würde.

**IX. Zusammenfassung in Thesen**

Auch wenn es für eine abschließende Beurteilung noch zu früh ist, weil das neue Instrument des verlässlichen Prüfpfades noch näher in der Praxis zu untersuchen sein wird, so wird eins offensichtlich klar: **Eine Vereinfachung der**

sichtspunkt die gesetzlichen Anforderungen und **bleibt strafbewehrt untersagt.**

- 2) Kein derzeit verfügbares Verfahren kann **alle gesetzlichen Anforderungen** an E-Rechnungen aus eigener Vollkommenheit erfüllen. Es bedarf somit immer einer angemessenen Kombination von verfügbaren Verfahren.
- 3) Ein verlässlicher Prüfpfad kann grundsätzlich durch interne Systeme i. S. d. GoBS und eine Papierspur erbracht werden, sofern eine Eignung für die Sicherheitsziele (Authentizität/Integrität/Lesbarkeit) auf **beiden Seiten der Kommunikation** dadurch gegeben ist.
- 4) In ständigen Geschäftsverbindungen können sich deutliche Vereinfachungen durch die Kombination von verlässlichem Prüfpfad, klassischen Verfahren

Ende der Vorschau

nung eher übervorsichtig und bedienen sich regelmäßig professionellen Rats.

Insofern können sich alle Verfahren nun einem echten Wettbewerb stellen und ihre Vorzüge ohne das „Dammoklesschwert“ des gesetzlichen Zwangs kommunizieren.

Thesen:

- 1) Der **ungeschützte Versand von E-Rechnungen** durch das Internet per E-Mail oder anders erfüllt auch in Zukunft m.E. unter keinem denkbaren Ge-

101 BMF-Rundschreiben vom 29. 1. 2004, IV B 7 - S 7280 - 19/04, hier insb. Rz. 70: „Bei elektronisch übermittelten Rechnungen hat der Unternehmer neben der Rechnung auch die Nachweise über die Echtheit und die Unversehrtheit der Daten aufzubewahren (z. B. qualifizierte elektronische Signatur), selbst wenn nach anderen Vorschriften die Gültigkeit dieser Nachweise bereits abgelaufen ist“.

102 „Die Rechnungen müssen für den gesamten Zeitraum die Anforderungen des § 14 Absatz 1 Satz 2 erfüllen.“

103 Die Signaturerneuerung wird entweder durch Übersignatur der Dokumente gem. § 6 Abs. 1 Satz 2 SigG, § 17 Satz 3 SigV i. V. m. § 2 Nr. 14 SigG oder mittels eines sog. Evidence Record gem. RFC 4998 gesichert. Letzteres Verfahren basiert auf einem Konsolidierungskonzept, das auf *Merkle* zurückgeht, vgl. *Merkle*: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, S.122–134, April 1980; in Deutschland bekannter unter der Bezeichnung Archisig/Archisafe-Projekt.