DURCHKLICK: ELEKTRONISCHE AKTENFÜHRUNG – BEWEISFÜHRUNG MIT EINGESCANNTEN DOKUMENTEN

LUKAS FÄSSLER
Rechtsanwalt und Informatikexperte, FSDZ Rechtsanwälte & Notariat AG, Zug

Stichworte: elektronische Aktenführung, Beweiswert eingescannter Dokumente

Auf dem Weg zur elektronischen Aktenführung stellt die Digitalisierung mittels Scanning der eingehenden Papierpost einen zentralen Prozess dar. Im elektronischen Dossier werden nur noch die eingescannten elektronischen Dokumente bearbeitet. Was geschieht mit den Papieroriginalen, und welchen Stellenwert kommt dieser Digitalisierung in der Beweisführung mit ersetzend gescannten Dokumenten zu?

I. Ausgangslage

Damit ersetzend gescannte Dokumente den Anforderungen an die Beweistauglichkeit und die Beweisführungssicherheit standhalten können, gilt es, einige wesentliche Gesichtspunkte zu berücksichtigen und in der internen Ablauforganisation sicherzustellen. Die allfällige Minderung des Beweiswertes gescannter Dokumente muss so gering wie möglich gehalten werden. Alle der Papierurkunde immanenten Merkmale gehen beim Scanvorgang verloren und können nach Vernichtung des Originals nicht mehr reproduziert und verwendet werden (z. B. Alter der verwendeten Tinte, Nachweis einer allfälligen Unterschriftsfälschung mittels forensischer Spezialanalysen etc.). Trotzdem steht einer Digitalisierung von Papieroriginalen im Bezug auf den Stellenwert in der Beweisführung grundsätzlich nichts entgegen, sofern gewisse Grundvoraussetzungen beachtet und bestimmte Massnahmen eingehalten werden. Letztlich unterliegt das gesamte Beweisverfahren weiterhin dem richterlichen Ermessen.

Immer mehr Unternehmungen gehen dazu über, eingehende Dokumente der Papierpost zu digitalisieren. Oft werden sie vorübergehend noch aufbewahrt, je länger, je mehr geht man aber dazu über, die Papieroriginale nach dem Scannen zu vernichten. Das vernichtete Papieroriginal wird durch sein digitales Abbild vollständig ersetzt. Das digitale Abbild muss später den beweisrechtlichen Anforderungen standhalten, die das bereits vernichtete Papieroriginal sicherstellen könnte. Das sogenannte «ersetzende Scannen» wird an Bedeutung gewinnen, da die Vorteile der elektronischen Aktenführung auf der Hand liegen[1] und zudem der Einsatz von Records-Management-Systemen oder elektronischen Dossierverwaltungssystemen nur noch elektronische Akten zulässt. Im Übrigen begünstigen die neuen prozessualen Bestimmungen über den elektronischen Geschäftsverkehr mit den Behörden und Gerichten die Digitalisierung der Papieroriginale. Kostenvorteile entstehen insbesondere dann, wenn die Aufbewahrung auf Papier in raumfressenden Archiven wegfällt und elektronische Akten überall und jederzeit für mehrere Benutzer gleichzeitig verfügbar sind.

Da ersetzend gescannte Dokumente im Streitfall von einer oder mehreren Prozessparteien im Sinne des Urkundenbeweises (auf Papier reproduzierte Kopien des digitalen Files als Abbild des Originals) in das Streitverfahren eingebracht werden können, dürften über kurz oder lang Fragen der Anfechtung der Beweisführung und die Bestreitung von Richtigkeit, Relevanz, Beweiskraft und Originalkonformität bei den Gerichten an Bedeutung gewinnen. Der nachfolgende Artikel will diesbezüglich auf einige wesentliche Aspekte eingehen, um die Beweistauglichkeit und die Beweisführungssicherheit ersetzend gescannter Dokumente zu erhöhen.

1 Beweisführung mittels ersetzend gescannter Dokumente; Dr. ALEXANDER ROSSNAGEL und wiss. Mitarbeiterin MAXI NEBEL, in: NJW 13/2014, S. 886.

II. Einleitung

1. Beweisführung in Prozessverfahren

In der Zivilprozessordnung (ZPO)[2] wird ausdrücklich festgehalten, dass elektronische Dateien selbst Urkunden sind (und nicht etwa nur Augenscheinsobjekte), selbst wenn die Sichtbarmachung technischer Geräte oder eines nachträglichen Ausdrucks bedarf.[3] Insbesondere wird auch auf die Beweistauglichkeit einer nicht im Original beigebrachten Urkunde eingegangen. Die ZPO erlaubt in Art. 180 ZPO ausdrücklich das Einreichen einer Urkunde in kopierter Form. Auch digitalisierte Dokumente und Kopien davon sind als Urkunden zugelassen (vgl. Art. 957 Abs. 4 OR; Art. 180 Abs. 1 ZPO). Dabei spielt es keine Rolle, ob es sich um genuin digitale Dateien oder bspw. um eingescannte Papierdokumente handelt.[4] Grundsätzlich trägt die Beweislast für die Echtheit einer Urkunde jene Partei, welche sich darauf beruft (Art. 8 ZGB). Dies bedeutet hingegen nicht, dass sich die Gegenpartei lediglich auf die Bestreitung der Echtheit beschränken kann. Vielmehr bedarf es einer substanziierten Bestreitung dieser Echtheit, welche berechtigte Zweifel an jener erwecken kann (Art. 180 Abs. 1 ZPO i. V. m. Art. 178 ZPO). Die Gegenpartei hat Tatsachen glaubhaft zu machen, welche Zweifel an der Echtheit der Urkunde oder der nachträglich erstellten Kopie eines eingescannten Dokumentes zu erwecken vermögen.[5] Nur in diesem Fall ist die beweisbelastete Partei verpflichtet, einen Echtheitsbeweis anzutreten.[6] Elektronische Urkunden oder Kopien aus eingescannten Dokumenten sind grundsätzlich genauso glaubwürdig wie Papierdokumente. Sie geniessen die Qualität eines Originals, wenn sie gewissen Standards entsprechen, insbesondere den handels- oder signaturrechtlichen Vorgaben (vgl. Art. 9 ff. GeBüV; Art. 14 Abs. 2 OR i. V. m. Art. 6 ff. ZertES). Die digitale Archivierung spielt in der Wirtschaft eine zunehmende Rolle und darf nicht zu einer beweisrechtlichen Benachteiligung führen.[7] Damit der Echtheitsbeweis erbracht werden kann, sind die nachfolgenden Ausführungen in Kapitel III von Bedeutung.

Im Strafverfahren ist der Urkundenbegriff i. S. v. Art. 192 Abs. 2 StPO nicht mit dem materiell-rechtlichen Urkundenbegriff nach Art. 110 Abs. 4 StGB identisch; massgebend ist der prozessrechtliche Begriff. Danach gilt als Urkunde jedes Schriftstück mit entsprechend gedanklichem Informationsgehalt. Unter weiteren Aufzeichnungen sind nicht schriftliche Aufzeichnungen mit dem vorerwähnten gedanklichen Informationsgehalt zu verstehen wie elektronischen Datenaufzeichnungen. Sie werden den Urkunden gleichgesetzt (Art. 192 Abs. 2 StPO).[8] Beweisgegenstände werden grundsätzlich im Original zu den Akten genommen (Art. 192 Abs. 1 StPO). Eine Ausnahme davon hat der Gesetzgeber in Art. 192 Abs. 2 StPO für Urkunden und weitere Aufzeichnungen statuiert: Sofern dies für die Zwecke des Verfahrens genügt, werden Kopien der Urkunden bzw. Aufzeichnungen erstellt und den Akten einverleibt.[9] Einzig wenn es auf die Beweiskraft des Originals selber ankommt, d. h., wenn die Urkunde bzw. die Aufzeichnung durch ihren Zustand oder ihre Beschaffenheit selber beweisbildend ist (z. B. gefälschte oder beschädigte Urkunden im Zusammenhang mit Urkundenfälschung nach Art. 251 ff. StGB), kann nur mit dem Original Beweis geführt werden.[10]

Im Verwaltungsgerichtsverfahren gelten in der Regel in der Beweisführung ähnliche oder die gleichen Vorschriften wie in der Zivilprozessordnung. Die Verwaltungsrechtspflegegesetze z. B. der Kantone ZG und BE verweisen in Art. 14 resp. Art. 19 für die Handhabung auf die Zivilprozessordnung. Das Verwaltungsrechtspflegegesetz des Kantons LU regelt die Originalkonformität einer Urkunde dahin gehend, dass nach Art. 66 VRG eine Kopie der Urkunde eingereicht werden kann, die Behörde jedoch die Beglaubigung oder das Original davon verlangen kann.

Entgegen der Botschaft zur ZPO kann ein Gericht das Original daher nicht nur dann verlangen, wenn der Prozess der Untersuchungsmaxime unterliegt, sondern auch in Verfahren mit Verhandlungsmaxime. Doch wird sich das Gericht in solchen Fällen in Zurückhaltung üben müssen, um nicht eine Partei ungerechtfertigt zu begünstigen.[11]

2. Standards und Stand der Technik

Im deutschen Recht fordern verschiedene spezialgesetzliche Bestimmungen,[12] beim Scannen den «Stand der Technik» sicherzustellen. Analog verweist in der Schweiz die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung, GeBüV) vom 24. 4. 2002 (SR 221.431) alle Buchführungspflichtigen in Art. 2 Abs. 3 GeBüV darauf, dass sich die Ordnungsmässigkeit der Führung und der Aufbewahrung der Bücher nach den anerkannten Standards zur Rechnungslegung richte. Werden die Geschäftsbücher elektronisch oder auf vergleichbare Weise geführt und aufbewahrt und die Buchungsbelege elektronisch oder auf vergleichbare Weise

2 Einschlägige Bestimmungen zu Beweisrecht, Urkunden und elektronischem Geschäftsverkehr insbesondere in Art. 150–193 ZPO, vorab Urkunden in Art. 177–180 ZPO und elektronischer Geschäftsverkehr in Art. 130 und 139 ZPO.

3 BSK ZPO-DOLGE (2. Auflage, Basel 2013): Art. 177 N 6; WEIBEL, in: Sutter-Somm/Hasenböhler/Leuenberger, ZPO-Komm., 2. Auflage, 2013, Art. 177 N 8.

4 Botschaft des Bundesrates zur Schweizerischen Zivilprozessordnung vom 28. Juni 2006 (nachfolgend. Botschaft ZPO), BBl 2006, 7221 ff., insbesondere 7322 f.; http://www.admin.ch/opc/de/federal-gazette/2006/7221.pdf.

5 BSK ZPO-DOLGE: Art. 178 N 2 ff.; WEIBEL, a. a. O., Art. 178 N 5 ff.

6 Botschaft ZPO, BBl 2006, 7221 ff., insbesondere 7322 f.; http://www.admin.ch/opc/de/federal-gazette/2006/7221.pdf.

7 Botschaft ZPO, BBl 2006, 7221 ff., insbesondere 7322 f.; http://www.admin.ch/opc/de/federal-gazette/2006/7221.pdf; BSK ZPO-DOLGE: Art. 177 N 11; WEIBEL, a. a. O., Art. 177 N 12 f.

8 BSK-StPO-BÜRGISSER (2011): Art. 192 N 5 und 8; DONATSCH, in: Donatsch/Hansjakob/Lieber, Kommentar zur Schweizerischen Strafprozessordnung, Art. 192 N 5 mit weiteren Verweisen auf die Botschaft des Bundesrates 2005c.

9 BSK-StPO-BÜRGISSER (2011): Art. 192 N 11; DONATSCH, a. a. O., Art. 1982 N 9.

10 BSK-StPO-BÜRGISSER (2011): Art. 192 N 11; DONATSCH, a. a. O., Art. 1982 N 9.

11 BSK ZPO-DOLGE: Art. 178 N 4 f.; WEIBEL, a. a. O., Art. 178 N 9 ff.

12 § 71 des E-Government-Gesetzes des Bundes vom 25. 7. 2013 (EGovG), BGBl. I 2013, 2749 und § 298a II deutsche ZPO.

erfasst und aufbewahrt, so sind die Grundsätze der ordnungsgemässen Datenverarbeitung einzuhalten (Art. 2 Abs. 2 GeBüV). Zudem dürfen gemäss Art. 9 Abs. 1 lit. b GeBüV zur Aufbewahrung von Unterlagen auch veränderbare Informationsträger (z. B. Harddisks etc.) verwendet werden, wenn u. a.

- technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten,
- der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z. B. durch «Zeitstempel»),
- die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie
- die entsprechenden Hilfsinformationen (wie Protokolle und Logfiles) ebenfalls aufbewahrt werden.

Der Gesetzgeber verweist somit in diesem von der technischen Entwicklung stark beeinflussten Umfeld auf anerkannte Normen und Standards sowie den Stand der Technik. In der Schweiz gibt es dazu – ausser den Bestimmungen in der GeBüV[13] – keine weiteren gesetzgeberischen Normen oder Standards. Es bleibt somit in der Verantwortung der Unternehmen – der Anwaltskanzlei –, nach eigener Risikobeurteilung die für eine ordnungsgemässe Beweisführung notwendigen Mindestmassnahmen bezüglich ersetzend eingescannten Dokumenten zu ergreifen. Hilfreich ist diesbezüglich immerhin die Technische Richtlinie 03138 «Rechtssicheres ersetzendes Scannen» (TR-RESISCAN) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI).[14] Die TR-RESISCAN enthält technische, organisatorische und personelle Anforderungen an Scanprozesse, die möglichst rechtssichere Scanlösungen ermöglichen und den Stand der Technik wie auch die Grundsätze ordnungsgemässen Scannens darstellen.[15] Dieser kommt heute wegen ihrer speziellen Auseinandersetzung mit der vorliegenden Materie die Rolle eines Quasistandards zu, welcher durchaus auch mit den Minimalanforderungen der GeBüV konform ist und praktisch umzusetzende und weiterführend konkrete Anforderungsparameter setzt.

3. Beweisführung im Allgemeinen

Die Reproduktion eingescannter Dokumente (oder deren Verwendung durch gerichtlichen Ausdruck, wenn eine elektronische Verfahrenseingabe erfolgte) entspricht der Kopie eines Papierdokumentes, die im Gerichtsverfahren ohnehin meist anstelle des Originals vorgelegt wird. Es bedarf also wohl spezifischer Beweiseinreden der Gegenpartei, wenn die Verlässlichkeit, die Integrität, die Originalkonformität oder der Beweiswert eines ersetzend gescannten Dokumentes in Zweifel gezogen werden will. Speziell ist einzig der Fall, wo beide oder mehrere Parteien unterschiedliche Scanprodukte des gleichen Originals vorlegen. Hier ist die Vermutung des Prozessbetruges gegeben, und die vorgelegten Kopien und die damit direkt verbundenen Scandateien bedürfen einer umfassenden technischen Analyse. Für den Beweiswert eingescannter Dokumente sind drei Stufen des Scannens[16] zu unterscheiden, die unterschiedlich gesichert und nachgewiesen werden können:

- Die Echtheit des Papierdokumentes kann nach dem Vernichten nicht mehr geprüft werden. Die in der materialisierten Beweisurkunde selber liegenden Beweismerkmale (Tinte, Alter des Papiers, spezifische forensische Analysen bezüglich der Unterschrift, der Datumsvergabe etc.) gehen verloren. In diesen Fällen kann das Vernichten des Originals zu Beweisnachteilen führen, wenn es ausnahmsweise wirklich einmal auf diese Merkmale ankommen sollte. Wichtige Urkunden sollten daher nach dem Scannen nicht vernichtet, sondern allenfalls an den Mandanten zur weiteren Aufbewahrung zurückgegeben werden.
- Die korrekte Übertragung des Originals in ein elektronisches Dokument kann nie unmittelbar bewiesen werden. Der sogenannte Medienbruch zwischen dem Original und der gescannten Datei liegt darin, dass nie mit absoluter Sicherheit durch den Scanvorgang selber bewiesen werden kann, dass wirklich das Original aufgelegt und gescannt worden ist. Der Übertragungsprozess kann und muss aber durch angemessene Organisationsanweisungen und deren Einhaltung plausibel gemacht werden. Dies kann durch (interne oder externe) Qualitätskontrollen, interne Prozessbeschreibungen, Mehraugenprüfungen mit schriftlicher Kontrollbestätigung, periodische interne Auditierung der vorgegebenen Prozesse mit schriftlichem Auditnachweis oder Scanning durch einen unbeteiligten Dritten (Outsourcingpartner) in einem dokumentierten oder sogar zertifizierten Scanverfahren sichergestellt werden. Je hochwertiger die Originale sind, welche ersetzend gescannt werden sollen, desto umfassender sollten die anzuwendenden Plausibilisierungsmethoden sein. Dies kann zu einer unterschiedlichen Handhabung des Scannings hinsichtlich des Stellenwertes von Originalen führen, welche wiederum durch eine Verfahrensanweisung schriftlich festzulegen ist.
- Schliesslich muss die Echtheit des gescannten elektronischen Dokumentes technisch gesichert und nachgewiesen werden können.

III. Massnahmen und Beachtungspunkte

Damit mit ersetzend eingescannten Dokumenten die notwendige Beweisführungssicherheit im Prozess- oder Verwaltungsverfahren erreicht werden kann und das richterliche Ermessen in der Beweiswürdigung genügend Argumente für die Zulassung und die Anerkennung des darin

13 Vgl. zudem den Verweis auf ElDI-V in Ziffer III/5 dieses Artikels.
14 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html.
15 ROSSNAGEL, a. a. O., S. 887.
16 Vgl. dazu auch die Ausführungen in ROSSNAGEL, a. a. O., S. 888.

wiedergegebenen Inhalts erhält, sind verschiedene Massnahmen und Beachtungspunkte umzusetzen.

1. Zeitpunkt des Scannens

Es wird empfohlen, den Zeitpunkt des Scannens nachweislich und möglichst unabhängig von eigenen Zeitmessinfrastrukturen zu dokumentieren. Es geht diesbezüglich vor allem darum, ein allfällig von der Gegenpartei unterschobenes Manipulationsinteresse zu zerstören. Entsteht ein allfälliges Manipulationsinteresse erst nach dem Scannen oder ergibt sich die Manipulationsmöglichkeit eindeutig erst danach, besteht an der Echtheit des Originals und an der Übereinstimmung zwischen Original und Scan kein Zweifel. Je früher ein Dokument gescannt wird, umso eher kann einem Manipulationsvorwurf begegnet werden. Systemzeitlogs eigener Infrastrukturen (eigener Server, eigener PC) sind aber nicht geeignet, diese Sicherheit herzustellen, da diese Zeitsysteme manipulierbar sind. Es wird empfohlen, elektronische Zeitstempel unabhängiger Anbieter von Zertifizierungsdiensten (Art. 2 lit. g ZertES, SR 943.03) zu verwenden. Auf entsprechendes Begehren müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten eine mit ihrer qualifizierten elektronischen Signatur versehene Bescheinigung abgeben, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen (Art. 12 ZertES). Andererseits können entsprechende Nachweise über Logdateien von Records-Management-Systemen (elektronische Dossierverwaltungssysteme) sichergestellt werden, sofern diese Systeme durch Dritte und nicht selber betrieben werden. Es dürfen aber keine Manipulationen an diesen Logdateien durch die Benutzer möglich sein (vgl. auch Art. 3 GeBüV). Scandateien müssen auch ohne Zwischenspeicherung direkt in das Dossierverwaltungssystem integrierbar sein.

In unserer Kanzlei verwenden wir dazu ein geschlossenes Scan-Archiv-Serversystem (Archivio-Server[17]) mit 2048-Bit-Verschlüsselung, welches bei jedem Scanvorgang das jeweilige Scanprodukt (elektronisches Dokument) im Format PDF/A generiert, verschlüsselt und automatisch mit einem nicht manipulierbaren Zeitstempel versieht. Es entspricht den höchsten Sicherheitsstandards und ist nach IDW PS880[18] zertifiziert (Institut der Wirtschaftsprüfer in Deutschland).

2. Nachbearbeitung

Ist die Qualität des Originals mangelhaft, stellt sich die Frage, ob durch Nachbearbeitungen der Scandatei beweisrechtliche Nachteile entstehen. Grundsätzlich bewirkt die Bearbeitung einer Scandatei mit den softwaremässig zur Verfügung gestellten Mitteln eines Scanprogrammes keine inhaltliche Veränderung. Dies gilt mindestens so lange, als keine Anhaltspunkte für eine Dateimanipulation bestehen. In den meisten Fällen führt eine Nachbearbeitung lediglich zu besserer Lesbarkeit (Schärfe) oder besserer Belichtung.

Aus beweisrechtlicher Sicht ist jedoch zu empfehlen, den Nachbearbeitungsvorgang, die ausführende Person und die dabei verwendete Software (Version) zu dokumentieren. Insofern ist ein Bildbearbeitungsprozess im Voraus und verbindlich zu dokumentieren. Zudem sollten die bearbeiteten Bilddateien mit einem Transfervermerk versehen und die bearbeitete Bilddatei wiederum mittels eines Zeitstempels signiert werden. In der Regel empfiehlt sich auch die Aufbewahrung der Ursprungsbilddatei sowie der neuen, bearbeiteten Bilddatei, um allfälligen Einwänden der Gegenpartei begegnen zu können.

3. Farbscan / Schwarz-Weiss-Scan

Grundsätzlich reicht für eine beweisrechtliche Darlegung des Inhalts des gescannten Originals eine s/w-Bilddatei. Diese braucht auch weniger Speicherplatz als eine Farbbilddatei. Hat die Farbe jedoch eine rechtliche Bedeutung (z. B. Bilanz- und Erfolgsrechnungen mit roten Zahlen für Negativwerte; Bilddateien von Autounfällen etc.), sollte das Original mittels Farbscan digitalisiert werden. Es ist also immer zu beurteilen, ob die Farbdarstellung von beweisrechtlicher Relevanz ist oder nicht. Ist der Scanvorgang an einen Drittdienstleister ausgelagert, bedarf es klarer Anweisungen, unter welchen Umständen anstelle eines standardmässigen s/w-Scans ein Farbscanning durchgeführt und bereitgestellt werden muss.

4. Scanprozessbeschreibungen

Da die wesentlichen Beweiseinreden darauf abzielen werden, die Originalkonformität einer aus einem ersetzend gescannten Dokument hergestellten Papierkopie oder der elektronisch eingereichten Scandatei anzugreifen, kommt der Dokumentation des im Unternehmen standardmässig und weisungsgemäss anzuwendenden Scanprozesses eine überragende Bedeutung zu. Eine solche Verfahrensdokumentation ist zwingend, wenn eine Unternehmung Originale in Papierform digitalisiert. Sie hat den Hauptzweck, in der Beweisführung die Einhaltung der einzelnen Scanprozessschritte nachzuweisen und damit die Angreifbarkeit der Originalkonformität ganz wesentlich zu minimieren. In einer solchen Verfahrensdokumentation wird somit die Korrektheit des Scannens indirekt plausibel gemacht, wodurch in Anspruch genommen werden kann, dass dieses Standardverfahren in allen angewandten Fällen immer dieselben Schritte durchläuft und somit einen hohen Grad an Sicherheit bei der Erstellung originalkonformer digitaler Abbilder des Papieroriginals garantiert.

Interessant ist in diesem Zusammenhang ein kurzer Blick in die TR-RESISCAN.[19] Die TR dient insgesamt als praxisorientierter Handlungsleitfaden für die Ordnungsmässigkeit eines Scanprozesses ohne eine damit verbundene Verpflichtung zur Zertifizierung. So führt die TR entlang eines strukturierten Scanprozesses die sicher-

17 http://www.bvlarchivio.de/produkt1.html.
18 http://www.ps880-softwarebescheinigung.de/html/software-bescheinigung.html.
19 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html.

heitsrelevanten technischen, personellen und organisatorischen Massnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammen. Dabei werden die Ziele der Informationssicherheit und der Rechtssicherheit gleichermassen berücksichtigt.[20]

Wer erstmals eine Verfahrensanleitung erarbeiten muss, findet insbesondere im Anhang 5[21] zur TR eine Mustervorgabe, welche mit den eigenen relevanten Anweisungen ergänzt werden kann. Allenfalls hilfreich kann auch noch der Verweis auf Art. 4 Abs. 1 GeBüV sein. Es geht auch hier darum, eine Risikoabschätzung für das eigene Unternehmen (die eigene Anwaltskanzlei) vorzunehmen und entsprechende Handlungsanweisungen zu formulieren.

So ist beispielsweise in der TR vorgegeben, dass zur Gewährleistung eines Höchstmasses an Beweistauglichkeit nach jedem Scanvorgang durch eine Drittperson die Scandatei nochmals am Bildschirm geprüft wird und diese Prüfung mittels einer zusätzlichen schriftlichen Originalkonformitätsbescheinigung und Unterschrift abzusichern sei, die wiederum eingescannt werden müsste. Wir haben mit der Durchsetzung dieser Verfahrensvorschrift in unserer Kanzlei natürlich und in gewissem Sinne verständlich grosse administrative Opposition hervorgerufen und uns daher darauf beschränkt, zwar die Qualitätskontrolle durch die einscannende Person sicherzustellen, aber nicht zusätzlich eine schriftliche Konformitätsbescheinigung zu erstellen und nochmals einzuscannen. Wir vermerken jedoch im erzeugten Filenamen der Scandatei durch Zufügen des Vermerks «okok» (z. B. /brief-20-07-2014_okok.pdf), dass die Qualitätskontrolle durch die scannende Person durchgeführt wurde (ok = Originalkonformität; ok = in Ordnung und geprüft). Unsere Risikobetrachtung hat ergeben, dass dies vorerst ausreichen sollte, jedoch eine Qualitätskontrolle unerlässlich ist (vgl. nachfolgend auch Ziff. 7). Denn insbesondere beim Scannen von zweiseitigen Dokumenten kann es vorkommen, dass durch Unachtsamkeit nur die aufliegenden Vorderseiten gescannt werden, was schliesslich in der digitalisierten Scandatei zur Unvollständigkeit führt, weil dann beispielsweise nur die Seiten 1, 3, 5 etc. gescannt werden, die Seiten 2, 4, 6 etc. jedoch fehlen. Eine solche Scandatei ist natürlich für die Beweisführung mittels eingescannter Dokumente später wertlos.

5. Stellenwert von Standards

Die mit dem Beweisverfahren befassten Gerichte suchen ebenfalls nach Rechtssicherheit und müssen in strittigen Situationen entscheiden, ob Beweismittel zugelassen werden oder nicht. Wird der Beweiswert oder die Beweistauglichkeit einer aus eingescannten Dokumenten reproduzierten Kopie oder einer elektronischen Scandatei von der Gegenpartei angezweifelt, liegt die Beweislast für die Originalkonformität, Authentizität, Identität, Unveränderthheit des Beweismittels bei der beantragenden Partei. Es obliegt somit ihr, mittels einer Kette von Argumenten und indirekten Plausibilitäten den Richter von der Originalkonformität ihrer aufgelegten Beweismittel zu überzeugen. Wer sich an Normen und Standards hält, ist schon mal wesentlich besser positioniert als eine Partei, die keine Standards anwendet, über keine Verfahrensdokumentation verfügt oder keine Qualitätskontrollen vorweisen kann.

Im Gegensatz zu Deutschland ist in der Schweiz noch keine der TR-RESISCAN ähnliche allgemeinverbindliche Norm oder Richtlinie für das ersetzende Scannen von Papieroriginalen bekannt. Dies wäre an sich eine interessante Aufgabe für die Schweizerische Normenvereinigung SNV[22], die in einem NK (Normen-Komitee) im interdisziplinären Bereich (INB) eine wertvolle diesbezügliche Grundlagenarbeit für die schweizerische Wirtschaft leisten könnte. Einzig in der Verordnung des EFD über elektronische Daten und Informationen (EIDI-V) vom 11. 12. 2009 (SR 641.201.511) regelt das Eidg. Finanzdepartement in Bezug auf die Mehrwertsteuer die technischen, organisatorischen und verfahrenstechnischen Anforderungen an die Beweiskraft und die Kontrolle von elektronisch oder in vergleichbarer Weise erzeugten Daten und Informationen (elektronische Daten) nach den Artikeln 122–124 MWSTV.

6. Interne Qualitätssicherungsmassnahmen

Organisatorische Massnahmen zur Sicherung der Qualität des Scanprozesses sind ein zentrales Mittel für die Nachvollziehbarkeit der Entstehung und die Beweistauglichkeit eines Scanproduktes. Dazu gehören u. a. stichprobenartige oder regelmässige Sichtkontrollen, welche einen Abgleich zwischen dem eingescannten Papieroriginal und der Scandatei vornehmen (vgl. dazu unsere Ausführungen unter Ziff. III/4). Wo jedoch Massenverarbeitungen stattfinden, ist eine individuelle Stichprobenkontrolle jedes einzelnen Dokumentes nicht mehr möglich. Hier muss eine angemessene (repräsentative) Stichprobenquote erreicht werden, welche natürlich abhängig vom Unternehmensrisiko (Risiko einer Nichtverwendbarkeit von Scandateien infolge Qualitätsmängeln) und abhängig vom unternehmerischen Schutzbedarf bezüglich der Dokumente abzuleiten ist.

Wo mehrere Personen, Abteilungen oder Konzernunternehmungen ein Beweisinteresse an einem Papieroriginal haben, muss die interne Qualitätskontrolle entsprechend höher gewertet werden. Für die Festlegung angemessener Stichprobenquoten kann allenfalls die Hilfe von Spezialisten (Statistiker, Bundesamt für Statistik; weiterführende Fachausführungen auch in: Prof. Dr. PETER VON DER LIPPE, Wie gross muss meine Stichprobe sein, damit sie repräsentativ ist?, Fachartikel Februar 2011;[23] BUNDESAMT FÜR STATISTIK, ZIMMERMANN, MORGENTHALER, HULLIGER: Die Stichprobe, warum sie funktio-

20 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html.
21 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html.
22 http://www.snv.ch.
23 http://www.von-der-lippe.org/dokumente/Wieviele.pdf.

niert, ISBN 3-303-00303-3[24]) in Anspruch genommen werden. Stichproben sind jedoch immer nur eine Momentaufnahme und dienen vorab dazu, systematische, wiederkehrende Fehler zu entdecken. Bleibt ein Fehler unentdeckt, geht dies immer zulasten des Beweisführers.

7. Scannen durch Dritte

Bei der Beurteilung der Frage, ob das Scanningverfahren im eigenen Unternehmen oder durch einen unabhängigen Dritten durchgeführt werden soll, kann u. a. auch in Betracht gezogen werden, dass im Rahmen der richterlichen Beweiswürdigung bei einem Scanning durch Dritte allenfalls weniger ein Manipulationsinteresse unterstellt werden kann. Der Dritte wendet seine Standardprozesse ohne jeden Bezug zu irgendwelchen inhaltlichen Aussagen im Papieroriginal einheitlich und für alle Dienstleistungsbezüger qualitativ gleich an. Er kann auch keineswegs beurteilen, welchen Stellenwert das jeweils zu scannende Papieroriginal dereinst für den Auftraggeber bekommen kann. Dem eigenen internen Scanprozess steht dieses Argument des fehlenden Manipulationsinteresses weniger zur Verfügung. Immerhin kann über den Faktor des Scanzeitpunktes (vgl. oben III/1) ein Argumentarium aufgebaut werden, welches das Manipulationsinteresse auf ein Minimum beschränkt.

Eine mögliche Lösung für das Scanning durch einen Dritten stellt die Post mit der Swiss Post Box zur Verfügung. Swiss Post Box ist das elektronische Gegenstück zum physischen Briefkasten. Die Post scannt die Briefsendungen ein und stellt diese in digitalisierter Form zur Verfügung.[25] Wie es sich mit dem Anwaltsgeheimnis, welches durch das Postgeheimnis ergänzt wird, im Einzelfall verhält, ist hier nicht zu klären, aber Aufgabe einer allenfalls auslagernden Anwaltskanzlei.[26]

8. Integritätsschutz

Der Nachweis der Echtheit und damit der Manipulationsfreiheit des Scanproduktes stellt sicher, dass ein Dokument von der angegebenen Person oder Unternehmung stammt und nicht nachträglich verändert worden ist. Dieser Integritätsschutz kann am besten systembezogen durch ein Records-Management-System oder Dossierverwaltungssystem sichergestellt werden, welches das Scanprodukt nachweislich unmittelbar und medienbruchfrei nach seiner Erzeugung ohne Eingriffsmöglichkeiten interessierter Dritter in das System integriert und diese Integration allenfalls zusätzlich noch in einem nicht durch Dritte manipulierbaren Logsystem protokolliert. Insbesondere wenn eine lückenlose Abfolge zwischen dem Scannen und dem Ablegen des Dokumentes keinen ungeschützten Zugriff auf die Datei zulässt, kann dem Einwand der Manipulation erfolgreich begegnet werden.[27]

Werden Scanfiles auch noch mittels elektronischer Signaturen digital signiert, würde eine Manipulation am signierten File sofort sichtbar und nachweisbar. Ob dafür eine fortgeschrittene elektronische Signatur eingesetzt wird, welche gemäss Art. 2 Lit. b ZertES[28] mit den Daten, auf die sie sich bezieht, so verknüpft wird, dass eine nachträgliche Veränderung der Daten sofort erkannt werden kann, oder ob dafür eine qualifizierte elektronische Signatur verwendet wird, die gemäss Art. 2 Lit. c ZertES auf einer sicheren Signaturerstellungseinheit nach Art. 6 Abs. 1 und 2 ZertES und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht (gemäss Art. 14 Abs. 2[bis] OR der eigenhändigen Unterschrift gleichgestellt), welches zusätzlich die Urheberschaft des Scanproduktes (Authentizität) garantiert, muss der einzelne Unternehmer/Anwalt entscheiden. Für den Integritätsschutz sind beide elektronischen Signaturen gleichwertig.

IV. Schlussfolgerungen

Das ersetzende Scannen von Dokumenten führt immer dann zu einem Verlust des Beweiswertes, wenn anhand der physischen Beschaffenheit des Papieroriginals oder darin enthaltener Elemente (Tinte, Zellulose etc.) Beweis geführt werden muss. Solche Papieroriginale sind aufzubewahren oder allenfalls nach dem Einscannen zur sicheren Aufbewahrung an den Mandanten zurückzugeben.

Mit ersetzend eingescannten Dokumenten lässt sich aber in Bezug auf den relevanten Inhalt jederzeit dann und in rechtsgenügender Form Beweis führen, wenn das Scanning des Papieroriginals möglichst früh erfolgt, auf einem geschlossenen, nicht von Dritten manipulierbaren Prozess beruht, eine möglichst direkte manipulationsgeschützte Integration des Scanproduktes in das Zielsystem (z. B. Records-Management-System oder Dossierverwaltungssystem) stattfindet, auf der Basis von nachweislichen Verfahrensvorschriften der Scanningprozess im Unternehmen/in der Anwaltskanzlei dokumentiert ist, sich an bekannte Standards und Normen anlehnt, die notwendigen Qualitätssicherungsmassnahmen angewendet werden, der Integritätsschutz durch den Einsatz von elektronischen Signaturen adäquat auf die Bedürfnisse des sicherzustellenden Beweiswertes des Scanproduktes ausgerichtet wird und allenfalls anstelle von im eigenen Unternehmen durchgeführten Scanprozessen eine Auslagerung an Dritte ins Auge gefasst wird. Letztlich obliegt es weiterhin der freien Beweiswürdigung des Gerichtes, wie im Beweisverfahren mit Einwänden in Bezug auf Richtigkeit, Relevanz und Beweiskraft (Originalkonformität) der Gegenpartei umgegangen wird. Das ist jedoch nicht anders als bei der bisher mehrheitlich geführten papierbezogenen Beweisführung.

---

24 www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CC8QFjAB&url=http%3A%2F%2Fwww.bfs.admin.ch%2Fbfs%2Fportal%2Fde%2Findex%2Fnews%2Fpublikationen.Document.61921.pdf&ei=CsHYU4Ihgc7RBYiAgYgN&usg=AFQjCNHjLg0esTbmxqeCBud8NipSlyOQsQ&sig2=9__34v7hKRvtZvk1KZcqNQ&bvm=bv.71778758,d.d2k.

25 http://www.post.ch/post-swisspostbox.

26 Der Autor dieses Artikels hat im Juli 2014 bei der Aufsichtskommission über die Rechtsanwälte des Kantons Zug eine entsprechende Abklärung über die Zulässigkeit der Inanspruchnahme des Swiss-Post-Box-Services eingeleitet.

27 ROSSNAGEL, a. a. O., S. 891.

28 Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur vom 19. Dezember 2003, SR 943.03.