

Damit elektronische Beweise nicht scheitern

Vollständige elektronische Abwicklung von Gerichtsverfahren ist Zukunftsmusik – aber schon heute kommen elektronische Dokumente als Beweismittel zum Einsatz.

VON RETO FANGER

Nach der Definition des Verbandes AIIM (Association for Information and Image Management) lässt sich der Umgang mit Unternehmensinformationen in fünf Lebenszyklen unterteilen: Erfassung (Capture), Verwaltung (Manage), Speicherung (Store), Bewahrung (Preserve) und Ausgabe (Deliver).

Dokumentenmanagement und Enterprise Content Management umfassen den gesamten Lebenslauf von Unternehmensinformationen und damit auch das Records Management (Aktenführung oder vorarchivische Schriftgutverwaltung) und die Archivierung (unveränderbare langzeitige Aufbewahrung). Grundsätze und Verfahren einer systematischen und umfassenden Aktenführung sind im internationalen Standard ISO 15489 normiert.

Generieren Unternehmen ihre Dokumente digital – seien dies originär digitale oder nachträglich digitalisierte Dokumente wie Scans – stellen sich gleichzeitig auch verschiedene Fragen im Hinblick auf allfällige Rechtsstreitigkeiten. Im Folgenden untersuchen wir daher, welche Anforderungen in zivilprozessualen Streitigkeiten, beispielsweise Forderungs- oder Haftungsprozessen, an digitale Dokumente zu stellen sind.

E-Litigation oder konventioneller Zivilprozess

Digitale Dokumente müssen im gesamten Lebenszyklus geeignet sein, Sachverhalte des Unternehmensalltags «gerichtsfest» zu beweisen, um allfällige Rechtsansprüche des Unternehmens durchsetzen oder ungerechtfertigte Gegenforderungen abzuschmettern.

Auch wenn der Weg zur E-Litigation, also zur vollständig elektronischen Abwicklung von Gerichtsverfahren, im schweizerischen Rechtsalltag noch weit ist – ein entsprechender Versuch des Bundesgerichts stiess in der Anwaltschaft auf wenig Interesse – gehört bereits heute die Beweisführung in konventionellen Zivilprozessen zu den Gebieten, in denen digitale Dokumente eingesetzt werden.

Was sind digitale Dokumente?

Ein digitales Dokument ist eine strukturierte Ansammlung digitaler Daten, die im Verlauf eines elektronischen Datenverarbeitungsprozesses

IN KÜRZE

- Für die Beweisführung in Zivilprozessen kommen bereits heute elektronische Dokumente zum Einsatz.
- Die Herausforderung liegt nicht in der Beweiseignung, sondern in der Beweiskraft der elektronischen Dokumente.
- Den höchsten Grad an Beweiskraft haben signierte Dokumente mit Zeitstempel.

zesses auf einem digitalen Datenträger aufgezeichnet wird, sich durch seine leichte Kopier- und Bearbeitbarkeit auszeichnet und sich nicht ohne technische Mittel für die menschliche Wahrnehmung wiedergeben lässt. Gegenstand eines digitalen Dokuments sind sämtliche Informationen, die sich in maschinell verarbeitbarer Form darstellen und auf Datenträgern festhalten lassen – formatierte Daten, unformatierte Daten, Bilddaten, Akustikdaten und Multimediadaten.

Als Datenträger dienen dabei magnetische Speichermedien wie Magnetstreifenkarte, Magnetband, Diskette oder Festplatte, optische und optomagnetische Medien wie WORM, CD, DVD oder Blu-ray und zunehmend auch rein elektronische Medien wie Flash-Speicherkarten, Chipkarten oder Solid State Disks.

Herausforderung Beweiskraft

Die Herausforderung bei der Beweisführung im Zivilprozess liegt nicht in der Beweiseignung digitaler Dokumente, sondern in deren Beweiskraft und dem damit korrelierenden Beweiswert: Je höher der Beweiswert, desto grösser die Beweiskraft.

Beweiswert und Beweiskraft eines Beweismittels bestimmen sich einerseits anhand formeller, rechtlicher Kriterien (Zulässigkeit im Rahmen der prozessualen Vorschriften), andererseits nach Massgabe der materiellen, inhaltlichen Zuverlässigkeit, soll doch das Gericht von einem bestimmten Sachverhalt überzeugt werden.



Rechtsanwalt Dr. iur. Reto Fanger ist Spezialist für IT-Recht.

Unproblematische formelle Zulässigkeit

Gestützt auf den Grundsatz des Rechts auf Beweis ist es in der Schweiz zulässig, in zivilprozessualen Verfahren mit digitalen Dokumenten Beweis zu führen. Nach den meisten kantonalen Zivilprozessordnungen sind digitale Dokumente mehrheitlich zu den Augenscheinobjekten zu zählen, vereinzelt sind sie auch dem Urkundenbeweis zuzurechnen.

Im Entwurf zur vereinheitlichten schweizerischen Zivilprozessordnung (ZPO), die sich zur Zeit in der parlamentarischen Beratung befindet und voraussichtlich im Jahre 2010 in Kraft treten soll, werden digitale Dokumente ausdrücklich den Urkunden zugerechnet werden, unabhängig von der Struktur der Daten und der Art des Datenträgers.

Digitale Dokumente können also bereits heute dem Gericht als Beweismittel vorgelegt werden, egal ob sie durch den Aussteller elektronisch signiert sind oder nicht. Die qualifizierte elektronische Signatur ist nach Art. 14 Abs. 2bis OR der Handunterschrift gleichgestellt und nur dann erforderlich, wenn der Abschluss eines Vertrags bewiesen werden soll, für dessen Zustandekommen das Gesetz die Schriftform in Abweichung des privatrechtlichen Grundsatzes der Formfreiheit ausnahmsweise voraussetzt (Art. 13 OR).

Unterschiedliche inhaltliche Zuverlässigkeit

Hinsichtlich der materiellen, inhaltlichen Zuverlässigkeit sind Echtheit und Wahrheit des digitalen Dokuments entscheidend. Die Beweiskraft digitaler Dokumente hängt von deren Authentizität (Aussteller) und Integrität (Unversehrtheit) ab. Während die Authentizität digitaler Dokumente einzig durch den Einsatz elektronischer Signaturen zuverlässig gewährleistet werden kann, hängt die Integrität teilweise auch von der Art des Datenträgers ab.

Digitale Dokumente, die auf überschreibbaren Datenträgern gespeichert sind, bieten naturgemäss keine Integritätssicherheit. Dazu gehören sämtliche magnetischen Datenträger, die rein elektronischen Datenträger wie Speicherkarten sowie einige optische Medien wie die CD-RW.

Bei Papierdokumenten sind nachträgliche Änderungen in der Regel von blossem Auge ersichtlich oder mittels spezieller Analyseverfahren feststellbar. Bei digitalen Dokumenten auf überschreibbaren Datenträgern trifft dies nicht zu. Änderungen können mehr oder weniger spurlos erfolgen, weil die körperlosen elektromagnetischen Spannungszustände unbemerkt manipulierbar sind.

So ist einerseits der Aussteller des digitalen Dokuments nicht erkennbar, und auch der Zeitpunkt der Erstellung bleibt unklar: Der Aufzeichnungszeitpunkt kann durch einfaches Verstellen der Systemzeit nachträglich manipuliert werden. Problematisch können auch Eingriffe Dritter sein, zum Beispiel durch gefälschte E-Mail-Absender, da sich bei dynamischen IP-Adressen die Rückverfolgbarkeit nur über den Provider bewerkstelligen lässt.

Manipulationssicherheit durch Signatur

Sind die digitalen Dokumente auf nicht überschreibbaren Datenträgern aufgezeichnet, können sie zumindest ab dem Aufzeichnungszeitpunkt nicht mehr manipuliert werden. Die Beweiskraft der nicht überschreibbaren Datenträger wie WORM, CD-R und DVD-R ist also von Natur aus höher als bei überschreibbaren Medien. Dennoch bleibt hier die Problematik bestehen, dass der Aussteller nicht erkennbar ist und über

den Zeitraum zwischen Erstellung des digitalen Dokuments und dessen Aufzeichnung nichts ausgesagt wird.

Den höchsten Grad an Sicherheit gegenüber Manipulationen und somit auch an Beweiskraft bieten elektronisch signierte Dokumente mit Zeitstempel, und zwar unabhängig von der Art des Datenträgers, auf dem sie aufgezeichnet sind. Einzig die elektronisch signierten Dokumente vermögen den Ursprung nachzuweisen und die Nichtabstreitbarkeit von Versand und Empfang zu garantieren. Zwar bietet auch die elektronische Signatur keinen vollständigen Schutz, allfällige Manipulationen lassen sich jedoch nachträglich eher nachweisen, weshalb die Beweiskraft eines signierten digitalen Dokuments vergleichbar mit derjenigen des herkömmlichen Papierdokuments ist.

Um die Beweiskraft elektronisch signierter Dokumente noch weiter zu steigern, sind sowohl technische Massnahmen wie der Einsatz von biometrischen Zugangssperren und Zeitstempeln als auch weitergehende organisatorische Massnahmen erforderlich, so die lückenlose Dokumentation des Zugriffs auf Systeme und Programme oder die Verwahrung bei vertrauenswürdigen Dritten.

Dementsprechend werden bei elektronischen Dokumenten, die auf überschreibbaren Datenträgern aufbewahrt sind, für die in Art. 957 Abs. 4 OR enthaltene Anknüpfung an die Beweiskraft der Papierurkunde weitere Integritätssicherungsmaßnahmen wie elektronische Signatur und Zeitstempel sowie eine zusätzliche Protokollierung verlangt. Dies wird in Art. 3 und 9 Abs. 1 lit. b GeBüV näher spezifiziert. Entsprechendes gilt für digitale Dokumente nach Art.

43 Abs. 1 MwStGV in Verbindung mit Art. 3 EIDI-V, auch wenn die identischen Sicherheitsmerkmale nach dieser Bestimmung zusätzlich noch den Nachweis des Ursprungs sowie die Nichtabstreitbarkeit von Versand und Empfang garantieren.

Folgen für das elektronische Dokumentenmanagement

Sollen digitale Dokumente über eine Beweiskraft verfügen, die den Papierdokumenten entspricht, bedürfen sie der gleichen inhaltlichen Zuverlässigkeit und Wahrheit. Daher sind im Hinblick auf eine allfällige Verwendung vor Gericht bereits in der aktiven Lebensphase (elektronische Aktenführung) dieselben Anforderungen an digitale Dokumente zu stellen, die gesetzlich im Rahmen der Buchführungsbestimmungen des OR sowie der Mehrwertsteuergesetzgebung eigentlich erst für die Aufbewahrungsphase (Archivierung) verlangt werden.

Nur so lässt sich letztlich garantieren, dass die Beweisführung vor Gericht nicht an der mangelnden Beweiskraft des digitalen Dokuments scheitert. Die Anbieter von elektronischen Dokumentenmanagementsystemen müssen deshalb auch für die aktiven Lebenszyklen eines digitalen Dokuments Lösungen anbieten, die Authentizität und Integrität sicherstellen können.

DR. IUR. RETO FANGER IST IN LUZERN ALS RECHTSANWALT MIT SCHWERPUNKT IT-RECHT TÄTIG UND UNTERRICHTET ALS LEHRBEAUFTRAGTER AN VERSCHIEDENEN HOCHSCHULEN. ER PROMOWIERT 2005 ZUM THEMA «DIGITALE DOKUMENTE ALS BEWEIS IM ZIVILPROZESS».

IM SCHWEIZERISCHEN RECHTSALLTAG IST DER WEG ZUR E-LITIGATION NOCH WEIT.