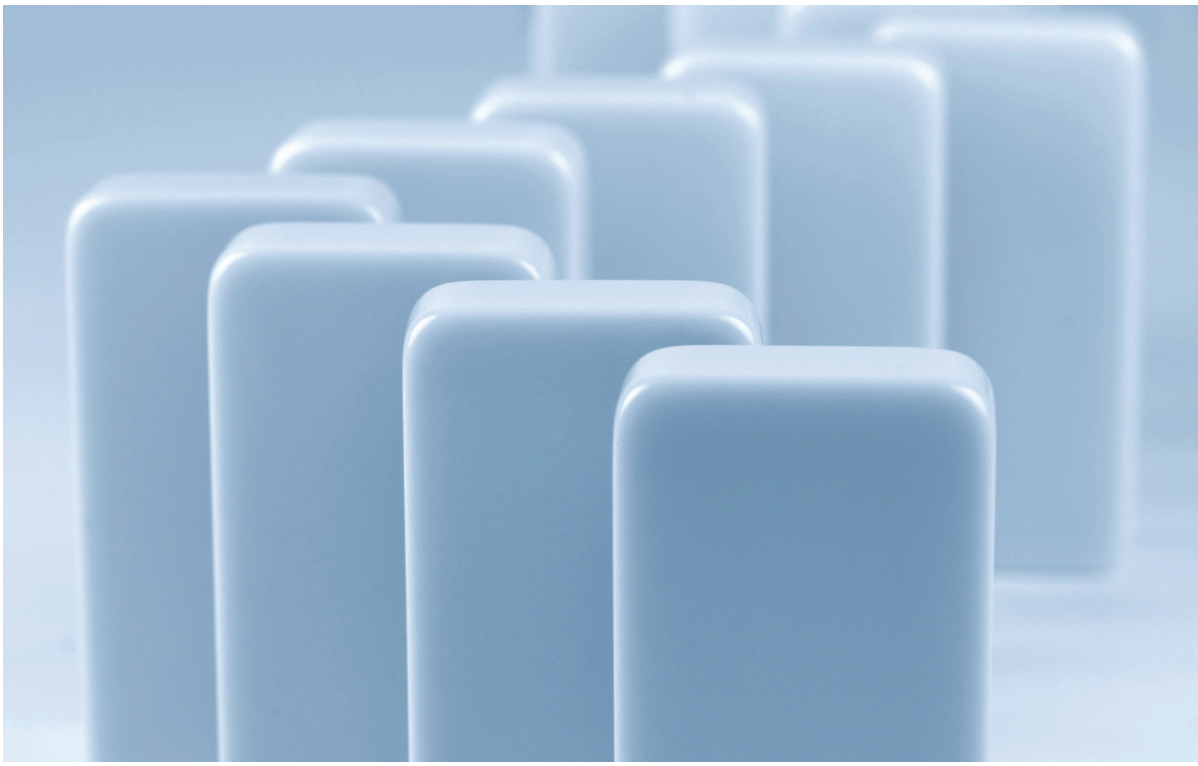
Deloitte.

Blockchain-Technologie
Revisionssichere Archivierung



Einleitung

Viele Unternehmen streben die elektronische Aufbewahrung von steuerrechtlich relevanten Dokumenten an. Allerdings sind sie unsicher, wie das dafür benötigte revisionssichere Aufbewahrungssystem ausgestaltet werden muss. Dieses Whitepaper gibt einen Überblick über die Hintergründe des Begriffs, welche Fallstricke bei der Ausgestaltung eines revisionssicheren Aufbewahrungssystems lauern, an welchem Stand sich Unternehmen technisch orientieren können und wie Blockchain-Technologie in einem revisionssicheren System eingesetzt werden kann.

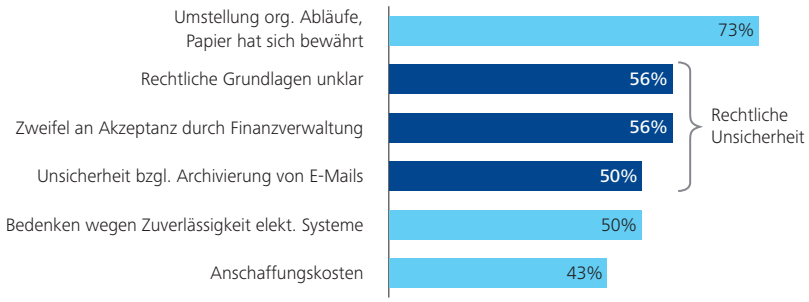
Grauzone Revisionssicherheit?

Als revisionssicher werden üblicherweise Systeme bezeichnet, mit denen es möglich ist, steuer- und handelsrechtliche Dokumente zu digitalisieren und elektronisch aufzubewahren. Die Mehrzahl der deutschen Unternehmen sieht deutliche Vorteile in der elektronischen Archivierung dieser Dokumente.[1] Dennoch bewahren die meisten Unternehmen steuerlich relevante Unterlagen in Papierform auf.[2] Als Hindernisse werden die Einführungskosten sowie rechtliche Unsicherheit genannt (s. Abb. 1).[3]

Die Unsicherheit beginnt bereits mit dem Begriff „Revisionssicherheit". Bei diesem handelt es sich nicht um eine rechtlich abgesicherte Definition, sondern um einen in den 1990er-Jahren vom Verband Organisations- und Informationssysteme (VOI) geprägten Terminus.[4] Im Kern geht es hierbei darum, die Integrität und Authentizität aller steuer- und handelsrechtlich relevanten Unterlagen über die gesetzlich vorgeschriebene Aufbewahrungsfrist zu wahren.[5] Integrität bezeichnet dabei den Nachweis, dass die Daten vollständig und unverändert sind, und Authentizität bezeichnet den Nachweis über die Echtheit der Daten und die eindeutige Zuordnung zum Verfasser.[6]

Um mehr Klarheit bzgl. der steuerrechtlichen Anforderungen zu schaffen, wurden im November 2014 die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[7] durch das BMF veröffentlicht. Sie können als Leitfaden für die revisionssichere Aufbewahrung dienen.

Abb. 1 – Rechtliche Unsicherheit ist einer der Hauptgründe, die Unternehmen an der Einführung einer elektronischen Aufbewahrung hindern



Hinderungsgründe für elektronische Aufbewahrung
Angaben in % der befragten Unternehmen

Quelle: Studie des Bundesministeriums der Finanzen

[1] Untersuchungsergebnisse des Projekts „Elektronische Archivierung von Unternehmensdokumenten stärken", 2014.

[2] Mit Ausnahme der Jahresabschlüsse, der Eröffnungsbilanz und bestimmter Zollunterlagen (siehe § 147 Absatz 2 AO) können steuerlich relevante Unterlagen elektronisch gespeichert werden. Dabei müssen Unternehmen sicherstellen, dass die Unterlagen mit dem Original bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.

[3] Eine Studie im Auftrag der EU-Kommission beziffert das europaweite, jährliche Einsparpotenzial durch e-Invoicing (elektronische Rechnungsstellung) auf ca. 64 Mrd. Euro., http://ec.europa.eu/finance/payments/einvoicing/index_de.htm

[4] Der VOI hat eine Orientierungshilfe zur gesetzeskonformen Ausgestaltung von DV-gestützter Buchführung veröffentlicht, zuletzt überarbeitet im Mai 2009.

[5] Die allgemeinen Grundsätze ordnungsgemäßer Buchführung gelten weiterhin.

[6] Die Zuordnung des Briefes zum ausstellenden Unternehmen (Authentizität) ist gemäß § 14 UStG über übliche Identifikatoren, z.B. den Briefkopf, ausreichend. Daher wird in diesem Whitepaper der Fokus auf die Integrität gelegt.

[7] Gültig seit dem 1. Januar 2015.

Welche Fallstricke lauern

Wie ein revisionssicheres Aufbewahrungssystem ausgestaltet wird, ist den Unternehmen überlassen. Üblicherweise dient das Aufbewahrungssystem nicht nur steuerlichen Zwecken, weitere Anforderungen an das System kommen hinzu. Folgende Punkte sollten berücksichtigt werden.

Beweiskraft

Revisionssichere Aufbewahrung adressiert im Allgemeinen die steuer- und handelsrechtlichen Anforderungen. Die Anerkennung vor Gericht kann mitunter höhere Anforderungen an die Handhabung von elektronischen Dokumenten stellen. Für Dokumente mit hohem Streitwert ist es empfehlenswert, sie nicht nur revisionssicher, sondern rechtssicher gemäß der technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu archivieren.

Vertraulichkeit

Dokumente können Betriebsgeheimnisse oder auch personenbezogene, vertraulich zu speichernde Daten enthalten. Je nach Grad der Vertraulichkeit müssen besondere organisatorische oder technische Maßnahmen ergriffen werden, um sicherzustellen, dass diese Daten nicht nach außen dringen.

Prozessgestaltung

Unternehmen erhalten relevante Dokumente auf unterschiedlichen Kanälen, seien es z.B. Eingangsrechnungen in Papierform, die in der zentralen Poststelle auflaufen, bis hin zu Reisebelegen, die jeder Mitarbeiter einzeln einreicht. Je nach Kanal kann eine zentrale oder dezentrale Erfassung der Dokumente sinnvoll sein, um den Prozess kostengünstig zu gestalten.

Insbesondere das ersetzende Scannen[8] von Papierbelegen stellt hohe Anforderungen an den Prozess. Lange Zeiträume zwischen dem Erhalt eines Papierdokuments und dessen Digitalisierung stellen den größten Risikofaktor für die Integrität der Dokumente dar. Ein zügiger, geordneter und dauerhaft überwachter Digitalisierungsprozess ist nötig, um die Beweiskraft der gescannten Dokumente zu erhalten.

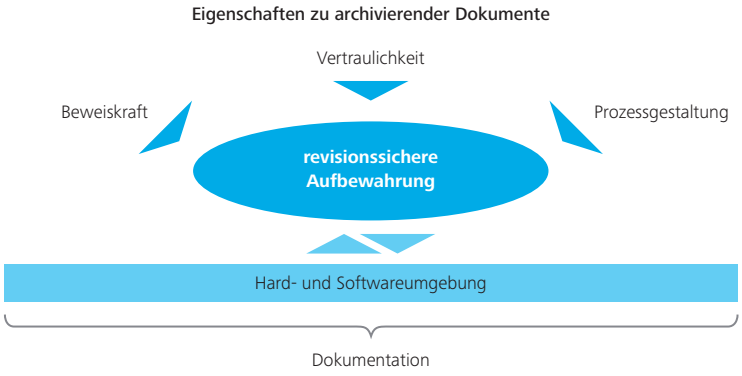
Hard- und Softwareumgebung

Den technischen Komponenten kommt insbesondere bei der Langzeitarchivierung hoher Stellenwert zu. Zum Beispiel kann die Unveränderbarkeit der Daten durch die Verwendung einmalig beschreibbarer Speichermedien, sogenannter WORM[9] Drives sichergestellt werden. Diese schließen aufgrund ihrer physikalischen Eigenschaften eine Änderung der darauf gespeicherten Daten aus. Neuere Systeme, wie z.B. CAS[10] Drives, nutzen Software, um die Eigenschaften der WORM Drives zu emulieren und gleichzeitig die Kostenvorteile von herkömmlichen Harddisk Drives auszuschöpfen.

Dokumentation

Alle unternommenen Maßnahmen müssen umfassend dokumentiert werden. Die Verfahrensdokumentation besteht typischerweise aus einer allgemeinen Beschreibung, einer Anwenderdokumentation, einer technischen Systemdokumentation und einer Betriebsdokumentation.[11] Weiterhin ist die Vorgehensweise bei der Datensicherung und die Beschreibung des betriebsinternen Kontrollsystems in der Verfahrensdokumentation zu beschreiben (s. Abb. 2).

Abb. 2 – Eckpunkte bei der Ausgestaltung eines revisionssicheren Aufbewahrungssystems



[8] Papierdokumente werden digitalisiert und anschließend vernichtet.

[9] Write Once Read Many.
[10] Content Addressable Storage.
[11] Vgl. auch Rz. 153 GoBD.

Orientierungshilfen: Stand der Technik

Die Richtlinien TR-03138 (RESISCAN) und TR-03125 (TR-ESOR) des BSI gelten als aktueller Stand der Technik für das ersetzende Scannen und die Langzeitarchivierung. Sie gehen über die Anforderungen der GoBD (bzw. Revisionssicherheit) hinaus.

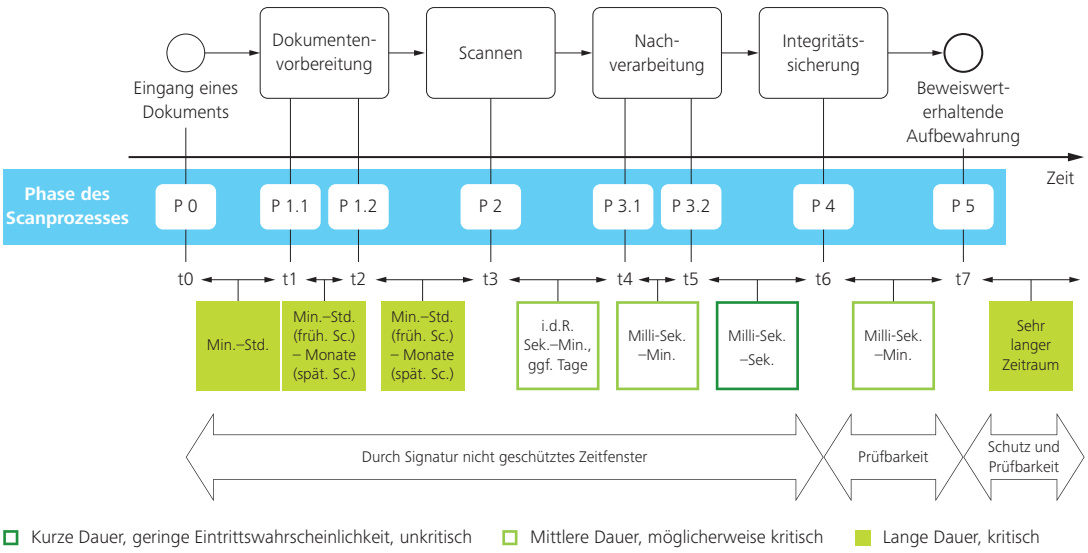
Die RESISCAN gibt einen modularen Baukasten vor, anhand dessen Unternehmen prüfen können, ob sie Papierdokumente rechtssicher digitalisieren.[12] Als wesentliche Bedrohung werden laut BSI längere Zeitabstände zwischen den einzelnen Prozessschritten des Scan-Prozesses gesehen. Insbesondere bei der Dokumentenvorbereitung können Fehler unterlaufen oder die zu scannenden Dokumente – willentlich oder unwillentlich – verfälscht werden, was zum Verlust der Integrität der Dokumente führt (s. Abb. 3).

Das Ziel von Unternehmen muss es sein, Dokumente zeitnah nach Erhalt zu scannen und zu verarbeiten. Für Dokumente, die an einer zentralen Stelle auflaufen (z.B. Eingangsrechnungen in der Poststelle), hat sich der zentrale Scan-Prozess etabliert. Dies hat den Vorteil, dass mit organisatorischen Maßnahmen (sprich Zugangsbeschränkungen) ausgeschlossen werden kann, dass Unbefugte Dokumente verfälschen. Weiterhin profitieren Unternehmen von effizienter Scan-Hardware und Skalierungseffekten. Für andere Belege (z.B. Reisebelege) ist ein zentraler Scanprozess ungeeignet, da dieser zusätzlichen Aufwand erfordert, um die Belege sicher an die zentrale Stelle zu bringen und über einen – häufig wochenlangen – Prozess die Integrität der Belege sicherzustellen.

Das Papieroriginal darf nach dem ersetzenden Scannen vernichtet und muss über die gesetzliche Aufbewahrungspflicht in elektronischer Form aufbewahrt werden. Die Aufbewahrungsvorschriften von HGB und AO sind dabei technikneutral und fordern lediglich die ordnungsmäßige Aufbewahrung, auch die GoBD geben kein spezielles technisches Verfahren vor.

Eine explizite technische Interpretation in Form einer Referenzarchitektur bietet hingegen das BSI in der TR-03125. Die dort skizzierte Lösung adressiert die beweiswerterhaltende Langzeitarchivierung von elektronisch signierten Dokumenten.[13] Der Kern der Referenzlösung ist die sogenannte Middleware, bestehend aus vier Komponenten, die als Zwischenschicht zwischen den Nutzeranwendungen und dem physischen Langzeitspeicher fungieren. Der Aufbau ist hierarchisch, an dessen Spitze befindet sich das ArchiSafe-Modul. Dieses regelt den Zugriff zum Langzeitspeicher, z.B. zu einem Enterprise-Content-Management-System, nach definiertem Berechtigungskonzept. Daneben zeichnet dieses Modul die Zugriffe zum Datenspeicher auf.

Abb. 3 – Kritische Prozessschritte im generischen Scan-Prozess (nach RESISCAN)



[12] Die Behörden des Bundes sind nach § 7 des EGovG angehalten, Dokumente elektronisch aufzubewahren. Die technische Richtlinie des BSI kann dabei als Stand der Technik referenziert werden.

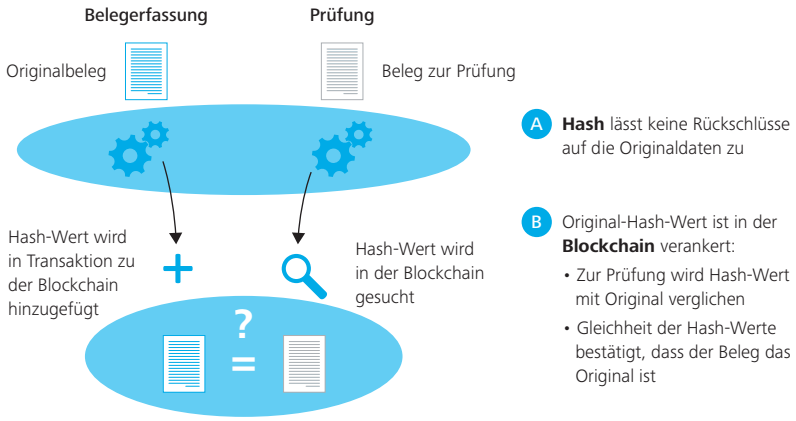
[13] Auch für Dokumente ohne elektronische Signatur kann diese IT-Architektur als technische Orientierung dienen.

Die darunter angesiedelten Module ArchiSig und das Krypto-Modul dienen der Erstellung und der laufenden Erneuerung elektronischer Signaturen. Die Signaturen dienen dem Abgleich der archivierten Dokumente mit ihrem Originalzustand und können so ungewollte Modifikationen aufdecken. Dieser Aufwand wird betrieben, um die Integrität bis zum Ende der Aufbewahrungsfrist aufrechtzuerhalten.

Mit der Blockchain die Integrität von Dokumenten wahren

Mit der Blockchain[14] kann die Integrität elektronischer Dokumente kostengünstig sichergestellt werden. Die Blockchain ist eine dezentral gespeicherte, unveränderbare und für jeden öffentlich zugängliche Datenbasis. Um die Integrität von E-Dokumenten zu sichern, kann ein elektronischer Fingerabdruck[15] des gescannten Dokuments erstellt und in die Blockchain geschrieben werden. So kann zu jedem späteren Zeitpunkt der Fingerabdruck der archivierten Datei mit dem in der Blockchain gespeicherten abgeglichen werden und – bei Übereinstimmung der Fingerabdrücke – die Integrität zweifelsfrei bewiesen werden (s. Abb. 4).

Abb. 4 – Integritätssicherung von elektronischen Dokumenten mit Blockchain



Beim Einsatz der Blockchain zur Integritätssicherung profitieren Unternehmen doppelt:

- Sie können einfache und bewährte Methoden nutzen, um elektronische Daten zu versenden (z.B. E-Mail), ohne die Integrität von Dokumenten zu gefährden; und
- sie können redundante Kontroll- und Validierungsprozesse minimieren.

Ausblick

Die Blockchain bietet eine bessere Alternative zu herkömmlichen IT-Komponenten bei der Sicherung der Integrität. Sie ist sicherer als lokale Methoden der Integritätssicherung, erspart Unternehmen den Aufwand, der durch das Signieren von Dokumenten entsteht, und kann flexibel in der bestehenden IT-Landschaft eingesetzt werden.

Integritätssicherung ist erst der Anfang. Auf Basis der Blockchain kann eine ganz neue, integre Dateninfrastruktur geschaffen werden. Sie kann in Zukunft als „goldene Quelle" für alle steuerlich relevanten Daten dienen und genutzt werden, um Prüfprozesse und steuerliche Erklärungen weitestgehend zu automatisieren.

Über die Autoren

Jannis Holthusen, Simon Kufeld und Florian Glatz sind die Gründer der Upchain GmbH. In Kooperation mit Deloitte entwickeln sie eine neue Datenplattform für aufbewahrungspflichtige Unterlagen auf Basis der Blockchain-Technologie. Damit können Unternehmen die Integrität ihrer Daten nachweislich sicherstellen und Prüf- und Kontrollprozesse stärker automatisieren.

[14] Vgl. auch das Whitepaper „Vorstellung der Blockchain-Technologie" für einen umfassenden Überblick über die Blockchain-Technologie.

[15] Vgl. kryptologische Hash-Funktion SHA-2, insbesondere SHA-512, http://www.nsrl.nist.gov/morealgs.html

Ihr Ansprechpartner

Nicolai Andersen
Partner, Leiter Innovation
Deloitte Deutschland
Tel: +49 (0)40 32080 4837
nicandersen@deloitte.de

Für weitere Informationen besuchen Sie unsere Website www.deloitte.com/de/blockchain

Stand 3/2016