YVES GOGNIAT

DIGITALISIERUNG DER TREUHANDBRANCHE

Praktische Hinweise, wie rechtliche Stolpersteine bei der Umsetzung umschifft werden können

Die Digitalisierung macht auch vor der Treuhandbranche nicht halt. Da der persönliche Kontakt und vor allem das Vertrauen für die Kunden sehr wichtig sind, wird der Treuhänder in nächster Zeit wohl noch nicht komplett durch einen Computer ersetzt werden. Im Vordergrund stehen vor allem Cloud-Lösungen. Bei richtiger Umsetzung können damit Kosten gesenkt und dem Kunden neue Arten der Kollaboration geboten werden.

Das Arbeitsumfeld hat sich in den letzten Jahren auch in der Treuhandbranche gewandelt. Der Einsatz von Cloud-Anwendungen hat Einzug gehalten in der Buchhaltung und bei den allgemeinen Treuhanddienstleistungen. Dabei steht vor allem *Software as a Service (SaaS)* im Vordergrund [1]. Diese Formel ermöglicht eine viel engere Zusammenarbeit mit dem Kunden, da mit der Nutzung einer gemeinsamen Plattform die Arbeitsteilung fliessend wird. Ausserdem wird dadurch die Umsetzung moderner Arbeitsformen wie Homeoffice, Mobileoffice usw. für (kleine) Treuhandunternehmen erschwinglich. Vielfach lassen es moderne IT-Lösungen zu, dass ein Kunde seinem Treuhänder oder der Treuhänder seinem Kunden jederzeit auf die Buchhaltung Zugriff geben kann. Dies vereinfacht den Informationsaustausch, führt aber gleichzeitig dazu, dass eine grössere gegenseitige Kontrolle möglich wird. Um mit einer Cloud-Anwendung ortsunabhängig arbeiten zu können, müssen auch alle Arbeitsunterlagen vorhanden sein, d. h. die Belege müssen in digitaler Form vorliegen. Auf die Digitalisierung von Belegen wird am Schluss dieses Beitrags eingegangen.

In der Praxis gibt es viele Schattierungen der Ausgestaltung des Auftrags des Treuhänders. Das Gleiche gilt für die Nutzung von IT-Services. Im Folgenden wird deshalb nur auf die Grundmodelle eingegangen.

1. ARBEITSAUFTEILUNG

Nachfolgend wird von folgenden Modellen der Arbeitsteilung bei Treuhanddienstleistungen ausgegangen:

YVES GOGNIAT, RECHTSANWALT, DIE ADVOKATUR SURY AG, LUZERN/ZÜRICH, LEHRBEAUFTRAGTER FÜR INFORMATIK- UND IMMATERIALGÜTERRECHT, ZÜRCHER HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN (ZHAW), WINTERTHUR/ZH

→ a) Der Treuhänder übernimmt die ganze Buchhaltung als Outsourcingprovider. D. h. der Kunde nimmt keine eigenen Buchungen vor. → b) Der Treuhänder übernimmt einen Teil der Buchhaltung – wie bspw. die Lohnbuchhaltung – und erstellt den Jahresabschluss. Der überwiegende Teil der Buchführung wird durch den Kunden selbst erledigt. → c) Der Treuhänder kontrolliert die Buchhaltung und erstellt für den Kunden den Jahresabschluss. → d) Der Treuhänder ist als Revisor tätig (wird nachfolgend nicht genauer behandelt). → e) Der Treuhänder ist für den Kunden als Steuerberater tätig (wird nur am Rande behandelt).

Zusätzlich darf nicht ausser Acht gelassen werden, dass der Treuhänder für KMU oft erster Ansprechpartner zu Fragen der Buchhaltung und Rechnungslegung ist. Er ist daher auch Vertrauensperson und somit zusätzlich Berater bei Fragen zu Buchhaltungs-, Rechnungslegungs- und Steuerfragen.

2. CLOUD-LÖSUNGEN

Im Folgenden wird der Fokus auf Cloud-Lösungen gelegt. Es wären auch Inhouse-Cloud-Lösungen denkbar, was für die meisten Treuhandunternehmen jedoch keine gangbare Lösung darstellt, da keine Skalierungseffekte realisiert werden können.

Was ist überhaupt unter dem Begriff Cloud zu verstehen? Die Cloud (Wolke) bzw. Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgt dabei ausschliesslich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software [2]. Beim Cloud Computing wird die Informatik nicht mehr selbst bereitgestellt und betrieben, sondern als Dienst bedarfsgerecht gemietet. Die Soft- und Hardware befindet sich nicht mehr im eigenen

Büro oder Serverraum, sondern in der Wolke. Die Cloud kann daher eine ganze Reihe von Dienstleistungen umfassen, die je nachdem wiederum von einer Vielzahl von Lieferanten oder Dienstleistern erbracht werden [3]. Allgemein gebräuchlich ist nachfolgende Dreiteilung:

1. *Infrastructure as a Service (IaaS):* Bei IaaS-Angeboten erhält der Nutzer Zugriff auf eine virtualisierte Infrastruktur und nutzt bereitgestellte Rechen- und Speicherkapazitäten. Der Anbieter ist dabei für den Zugang und die genutzte Infrastruktur, der Nutzer für die verwendete Applikation verantwortlich.
2. *Plattform as a Service (PaaS):* Diese Variante einer Cloud ermöglicht dem Nutzer (wie z. B. Softwareentwicklern), auf der Infrastruktur des Anbieters eigene Programme zu entwickeln und auszuführen. Der Anbieter macht hierbei Vorgaben zu den verwendeten Programmiersprachen und Schnittstellen zu Datenspeichern, Netzwerken und Datenverarbeitungssystemen.
3. *Software as a Service (SaaS):* Im Gegensatz zu allen anderen Angeboten werden beim SaaS dem Nutzer standardisierte Anwendungen zur Verfügung gestellt, die auf der Infrastruktur des Anbieters gespeichert sind. Auf deren Ausgestaltung kann der Nutzer zwar nur in geringem Mass Einfluss nehmen. Dafür erhält er eine sofort nutzbare Anwendung ohne eigenen Aufwand für deren Pflege und Unterhalt [4].

In Bezug auf die Dienstleistungen von Treuhändern steht die Nutzung einer Cloud in einem Dreiecksverhältnis zwischen dem Cloud-Anbieter, dem Treuhänder und dem Kunden. Dabei sind vereinfacht folgende Varianten denkbar, wobei es natürlich in der Praxis immer wieder verschiedene Schattierungen geben kann:
→ 1. Der Treuhänder nutzt IaaS des Cloud-Anbieters nur als externe Ablage, die Software wird weiterhin lokal betrieben; oder er installiert diese selbst in der Cloud. → 2. Der Treuhänder nutzt IaaS des Cloud-Anbieters als umfassende Infrastruktur und lässt sich einen virtuellen Arbeitsplatz inklusive Softwarelösung bereitstellen. → 3. Der Treuhänder erledigt die komplette Buchführung für einen Kunden und setzt dafür Variante 1 oder 2 ein (Outsourcing der Buchhaltung). → 4. Der Treuhänder arbeitet direkt mit der Cloud-Lösung des Kunden, es können beide darauf zugreifen. → 5. Die beim Kunden eingesetzte Cloud-Anbieter-Lösung als SaaS wurde vom Treuhänder empfohlen.

Bei der Nutzung der Cloud gibt es ebenfalls diverse Schattierungen, wie die Technologie genutzt werden kann. In Anleh-

nung an die obige Eingrenzung wird nicht auf jede Variation eingegangen.

3. AUSWAHL CLOUD-ANBIETER

Mittlerweile gibt es eine Vielzahl von Cloud-Anbietern. Es kommt darauf an, wie man die Cloud nutzen möchte. Möchte man die ganze IT-Infrastruktur in die Cloud auslagern und nur noch mit virtuellen Clients arbeiten, ist ein anderer Anbieter zu wählen als für die Auslagerung eines Buchhaltungssystems. Ersterer nimmt einem zwar den ganzen Unterhalt ab, wird aber meist nicht gleichzeitig eine eigene Buchhaltungssoftware anbieten. Die Buchhaltungssoftware wird also weiterhin bei einem Dritten zu besorgen sein. Dabei gibt es zwei Varianten: Die Buchhaltungssoftware wird wie bis anhin als Software lizenziert, nur wird diese jetzt beim Cloud-Anbieter installiert und nicht mehr lokal. Dabei ist zu prüfen, ob die entsprechende Software in einer Cloud-Umgebung lauffähig und ob dafür allenfalls eine spezielle Lizenz notwendig ist. Bei der zweiten Variante wird über den (virtuellen) Arbeitsplatz auf die SaaS-Version eines Buchhaltungsanbieters zugegriffen. Vor allem wenn ein virtualisierter Arbeitsplatz genutzt wird, ist sicherzustellen, dass der Internetprovider genügend Bandbreite bieten kann. Da es so viele Schattierungen bei der Nutzung gibt, sind vorgängig die eigenen Bedürfnisse genau zu analysieren, um eine bedürfnisgerechte Auswahl treffen zu können.

4. VERTRAGSGESTALTUNG

Cloud-basierte Anwendungen können sehr vielseitig sein. Ebenso vielfältig sind die vertraglichen Regelungsmöglichkeiten, die von zu bestätigenden allgemeinen Nutzungsbedingungen per Mausklick bis hin zu massgeschneiderten Vertragswerken reichen [5]. Gerade bei grösseren Anbietern ist der Spielraum für individuelle Verhandlungen sehr klein. Nichtsdestotrotz gilt es, die Vertragsbedingungen im Vorfeld genau zu prüfen. Nur so kann festgestellt werden, ob die eigenen Bedürfnisse alle abgedeckt sind. Nachfolgend werden einige wesentliche Punkte genauer betrachtet.

4.1 Leistungsgegenstand. Der Umschreibung der vertraglichen Leistung kommt beim Cloud-Service-Vertrag elementare Bedeutung zu. Wie bereits oben festgehalten, können im Einzelfall sehr unterschiedliche Leistungen vereinbart werden. Bei gemischten Innominatkontrakten, zu denen auch der Cloud-Service-Vertrag zählt, bereitet die Orientierung an einem vom Gesetzgeber geregelten Vertragstypus Probleme. Deshalb müssen die zu erbringenden Leistungen im Vertrag detailliert und präzise umschrieben werden [6]. Die Parteien haben insbesondere zu regeln, welche wiederkehrenden Leistungen anhand welcher Leistungskriterien zu erbringen sind, wie die Leistungserbringung kontrolliert wird und was die Konsequenzen bei Nichteinhaltung der Leistungskriterien sind [7]. Je mehr Aufgaben ein Unternehmen an einen Cloud-Anbieter auslagert, desto abhängiger macht es sich von diesem. Im schlimmsten Fall steht das Treuhandbüro bei einem Ausfall still. Von besonders grosser Bedeutung ist deshalb die Regelung der Verfügbarkeit [8] des vereinbarten Service und der Störungsbehebungszeiten.

4.2 Migration. Da die wenigsten Treuhänder bei null starten, gilt es unbedingt, die Migration bestehender Daten bei Vertragsbeginn zu regeln. Es ist sicherzustellen, dass bei der Datenübertragung keine Daten verloren gehen. Dies vor allem dann, wenn mit der Auslagerung gleichzeitig ein Wechsel des Enterprise Resource Planning (ERP; Planung und Steuerung der Unternehmensressourcen wie Kapital, Personal, Betriebsmittel, Material und IT mithilfe eines IT-Systems) erfolgt. Für einen Treuhänder ist es zudem essenziell, dass er allen gesetzlichen Aufbewahrungspflichten nachkommen kann. Eine Möglichkeit besteht darin, den Wechsel auf den Jahresbeginn zu legen, sodass viele Datenübertragungen eingespart werden können. Müssen oder sollen trotzdem Daten übertragen werden, ist die Kompatibilität der Datenformate sicherzustellen. Ebenso sind die benötigten Unterstützungsleistungen des Cloud-Anbieters und die damit verbundenen Kosten zu klären.

Durch die Nutzung des Cloud-Service begibt sich der Treuhänder in eine grosse Abhängigkeit zum Cloud-Anbieter. Am Ende des Vertragsverhältnisses ist der Treuhänder deshalb darauf angewiesen, dass er wieder sämtliche Daten in einem Format und in einer Struktur zurückerhält, die es ihm ermöglicht, seine Treuhändertätigkeit nach Vertragsbeendigung ohne grössere Probleme weiterzuführen oder den Anbieter zu wechseln. Im Vertrag sollte sich der Treuhänder daher die benötigte Unterstützung bei der Übertragung der Daten nach Beendigung des Vertragsverhältnisses ausbedingen. Es gilt zu definieren, welche Arbeiten der Anbieter kostenlos zu erbringen hat und welche extra vergütet werden müssen. Zusätzlich sollte darauf geachtet werden, ob solche zusätzlichen Arbeiten zu den üblichen Ansätzen erbracht werden oder nicht. Da der Cloud-Anbieter nach Beendigung des Vertrags kaum noch über Preise verhandeln wird, sind angemessene Konditionen im Vorfeld zu vereinbaren. Darüber hinaus sollte der Cloud-Anbieter dem Treuhänder für eine bestimmte Zeit nach Vertragsbeendigung für Fragen zur Verfügung stehen [9].

4.3 Change Management. Cloud-Computing-Verträge erstrecken sich meist über eine längere Zeitspanne. Die Bedürfnisse der Parteien lassen sich meist nicht gleich von Beginn weg abschliessend definieren. Zudem können sich die Anforderungen an die zu erbringenden Leistungen während der Vertragslaufzeit verändern. Aus diesem Grund sollten im Vertragswerk Regelungen für spätere Vertragsanpassungen vorgesehen werden.

In Bezug auf Treuhanddienstleistungen gilt es, vor allem den regulatorischen und gesetzlichen Änderungen besondere Beachtung zu schenken. Wer ist bei gesetzlichen Änderungen für Anpassungen an der Software verantwortlich? Wird dies nicht vorgängig geregelt, kann daraus schnell eine Streitfrage entstehen, da sich niemand verantwortlich fühlt. Es ist deshalb festzulegen, welche Vertragspartei für welche Änderung verantwortlich ist. Die Parteien sollten regeln, welche Änderungen autonom vollzogen werden können, also ohne zusätzliches Tätigwerden bzw. ohne Einwilligung der anderen Partei. Solche automatischen Anpassungen können etwa für den Fall gesetzlicher Änderungen oder anderer klei-

nerer Veränderungen vorgesehen werden (bspw. Anpassen MWST-Sätze).

Des Weiteren sollte für Änderungen, für die keine automatische Anpassung vorgesehen ist, klar geregelt sein, ob es sich um einen kostenpflichten Change handelt oder dies bei den regelmässigen Updates inbegriffen ist. Allgemein ist ein Change-Management-Verfahren vorzusehen. Bei einem solchen Verfahren steht es beiden Seiten offen, Leistungsänderungen zu beantragen. Die Partei, bei welcher der Änderungsantrag eingeht, hat dann innert einer vereinbarten Frist der beantragenden Partei auf das Änderungsbegehren zu antworten. Zusätzlich sollte ein Eskalationsverfahren vorgesehen werden. Dieses kommt für den Fall zur Anwendung, dass sich die Parteien im Rahmen des Change-Management-Verfahrens nicht einigen können.

4.4 Lizenzierung. Ein wichtiges Thema bei der Nutzung von Cloud-Services sind die Lizenzen. Nur schon beim Wechsel von einer lokal installierten Software zur Cloud-Lösung stellt sich die Frage, ob dies eine Änderung der Lizenz nach sich zieht. Um eine Lizenz für mehrere Kunden nutzen zu dürfen, reicht eine einfache Lizenz nicht aus. Deshalb muss der Treuhänder abklären, wie viele Mandate mit einer Lizenz eröffnet werden können. Je nach Bedürfnis drängen sich unterschiedliche Lizenzmodelle auf, beispielsweise das Concurrent-User-Lizenzmodell [10] oder das Named-User-Lizenzmodell [11]. Auch die Ausgestaltung der Lizenzen kann sehr unterschiedlich ausfallen. So kann vereinbart werden, dass neben dem Treuhänder auch der Kunde auf die lizenzierte Software zugreifen kann, was allenfalls zu höheren Lizenzkosten führt. Sofern ein Kunde nur Einsicht in seine verarbeiteten Unterlagen oder seine Buchhaltung haben möchte, gilt es, die Möglichkeit einer View-Only-Lizenz zu prüfen, um nicht teure Volllizenzen kaufen zu müssen.

4.5 Kosten. Typischerweise werden für Cloud-Services nutzungsabhängige Vergütungsmodelle (pay as you go) vereinbart. Möglich ist allerdings auch eine Abrechnung pro Benutzer und Monat [12], was bei Treuhandlösungen meist der Fall ist.

5. DATENSCHUTZ

5.1 Datenbearbeitung. Sobald eine private Person innerhalb einer Cloud Daten von natürlichen oder juristischen Personen bearbeitet, ist das Datenschutzgesetz anwendbar. Im Rahmen der Buchführung werden immer Personendaten bearbeitet, da bereits der Name und die Adresse als Personendaten gelten. Im Dezember 2016 wird der Entwurf des revidierten Datenschutzgesetzes erwartet. Wahrscheinlich wird darin vorgeschlagen, dass juristische Personen in Zukunft nicht mehr unter das Datenschutzgesetz fallen [13]. Dadurch würden in Zukunft viele Personaldatenbearbeitungen wegfallen, da die meisten B2B-Transaktionen nicht mehr unter das Datenschutzgesetz fallen würden.

Gemäss Art. 4 und Art. 5 des *Datenschutzgesetzes (DSG)* müssen bei jeder Datenbearbeitung die Grundsätze des Datenschutzes respektiert werden. Personendaten müssen rechtmässig erhoben werden, was unproblematisch sein sollte [14]. Die allermeisten Personendaten werden von den Kunden an den Treuhänder weitergeleitet, womit die Verantwortung grundsätzlich beim Kunden liegt. Stellt ein Treuhänder einen Verstoss fest, hat er dies dem Kunden mitzuteilen, denn das fordert die auftragsrechtliche Sorgfaltspflicht.

Die Personendaten müssen nach Treu und Glauben bearbeitet werden. Sie dürfen nur zum Zweck bearbeitet werden, der bei der Beschaffung angegeben worden, der aus den Umständen ersichtlich oder der gesetzlich vorgesehen ist [15]. Auf die Buchhaltung bezogen ist die Einhaltung dieser Grundsätze unproblematisch. Zum einen besteht eine gesetzliche Pflicht zur ordentlichen Buchführung, zum anderen erfolgt die Bearbeitung meist im Rahmen der Vertragsabwicklung. Das Risiko eines Verstosses beziehungsweise eines absichtlichen Fehlverhaltens der Mitarbeiter ist insofern reduziert, als diese meist dem Berufsgeheimnis unterliegen. Die Standesregeln [16] verpflichten ebenfalls zur Verschwiegenheit.

5.2 Datenbearbeitung durch einen Dritten. Befinden sich die Personendaten in der Cloud, muss der Cloud-Anbieter ebenfalls in die Pflicht genommen werden. Das Speichern von Personendaten auf einer Cloud stellt eine sogenannte Datenbearbeitung durch Dritte dar. Das Auslagern von Daten in die Cloud ist nach Art. 10a DSG grundsätzlich zulässig, und zwar ohne Einwilligung der betroffenen Personen. Die Daten dürfen aber nur so bearbeitet werden, wie es der Kunde bzw. Treuhänder selber tun darf, auch das nur, solange keine gesetzliche oder vertragliche Geheimhaltungspflicht die Bearbeitung durch einen Dritten verbietet. Es muss ausserdem sichergestellt werden, dass der Cloud-Anbieter die notwendigen Voraussetzungen für eine datenschutzkonforme Datenbearbeitung erfüllt und insbesondere die Datensicherheit gewährleistet ist. Eine sorgfältige Auswahl des Anbieters ist deshalb zwingend und eine vorgängige Prüfung des Anbieters auf die Einhaltung des Datenschutzes wichtig. Zusätzlich muss der Cloud-Anbieter entsprechend instruiert werden, insbesondere über den erlaubten Zweck und den Umgang der Datenbearbeitung sowie die einzuhaltenden Sicherheitsstandards. In Bezug auf die Datenbearbeitung sollte ein Weisungsrecht ausbedungen werden [17]. Im Aktivbetrieb gilt es zudem, den Anbieter zu überwachen, da sonst auch der beste Vertrag nicht viel hilft.

Es darf nicht vergessen werden, dass der Cloud-Anbieter nur Hilfsperson ist und die Haftung nicht auf ihn abgewälzt werden kann. Deshalb ist es wichtig, dass für alle Parteien klar ist, wer den Cloud-Anbieter beauftragt hat. Wird der Cloud-Anbieter durch den Kunden direkt beauftragt und nutzt ein Treuhänder lediglich die Infrastruktur des Kunden, liegt es grundsätzlich in der Verantwortung des Kunden, den Datenschutz gemäss Art. 10a DSG zu regeln. Der Treuhänder hat sich ebenfalls an die Vorgaben des Kunden zu halten und ist in dieser Konstellation Auftragsdatenbearbeiter. Anders sieht die Sache aus, wenn der Treuhänder selbst einen Vertrag mit einem Cloud-Anbieter abschliesst. Da er bereits Auftragsdatenbearbeiter ist, hat er sicherzustellen, dass auch seine Serviceprovider die vorgeschriebenen Datenschutzbestimmungen einhalten.

5.3 Bearbeitung im Ausland. Zunächst ist festzuhalten, dass das DSG keine eigene Bestimmung zum örtlichen Geltungsbereich enthält. Aufgrund seines grundsätzlich öffentlich-rechtlichen Charakters findet deshalb auf die datenschutzrechtlichen Gebote und Verbote zunächst das Territorialitätsprinzip Anwendung [18]. Ein Outsourcing ins Ausland ist nur zulässig, wenn ein vergleichbarer Datenschutz gewährleistet werden kann. Ansonsten ist ein spezieller Outsourcing-Vertrag abzuschliessen, in welchem sich der Dritte zur Einhaltung des Datenschutzes verpflichtet (Art. 6 DSG) [19]. Eine Übersicht über das Datenschutzniveau der verschiedenen Länder findet sich auf der Webseite des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) [20]. Neben dem Datenschutz gilt es aber, auch die gesetzlichen Sonderregelungen oder vertraglichen Geheimhaltungsverpflichtungen zu berücksichtigen. Ein Treuhänder unterliegt bei gewissen Tätigkeiten dem Berufsgeheimnis, weshalb ein Outsourcing ins Ausland meist einer expliziten Zustimmung bedarf. Zudem kann nicht ausgeschlossen werden, dass eine ausländische Behörde plötzlich über den Cloud-Anbieter auf Kundendaten zugreift [21]. Soll dieses Risiko vermieden werden, ist ein Schweizer Anbieter zu wählen. Bei der Entscheidung für einen ausländischen Anbieter muss die Verfügbarkeit der Daten jederzeit gewährleistet sein; dies fordert das Steuerrecht [22], aber auch andere Sondervorschriften wie bspw. die Geldwäschereivorschriften [23].

6. DATENSICHERHEIT

6.1 Sicherheit der Cloud-Lösung. Wie oben ausgeführt, muss Sicherheit in Bezug auf die Daten bestehen [24]. Dies kann vertraglich geregelt und durch Überprüfen der Reglemente und Prozesse des Cloud-Anbieters sichergestellt werden. Fehlt das Wissen für eine Vertragsprüfung, sollte auf einen externen Rechtsexperten zurückgegriffen werden. Eine technische Sicherheitsprüfung ist normalerweise zu komplex für einen Treuhänder. In diesem Fall bietet sich der Beizug eines Informatikspezialisten an, um sicherzugehen, dass die notwendigen Sicherheitsmassnahmen (Firewall, Anti-Virus-Programm, Verschlüsselung) vorhanden und auf dem neusten Stand sind. Zudem ist ein solcher Spezialist besser in der Lage, die fachliche Kompetenz eines Anbieters zu prüfen. In welchem Umfang ein solches Sicherheitsaudit möglich ist, hängt meist stark von der Grösse eines Cloud-Anbieters ab. Bei Grossanbietern wird ein eigenes Auditrecht oft nicht möglich sein. Manchmal wird aber auf Nachfragen Zugang zu entsprechenden Auditberichten gewährt. Ein weiteres Qualitätsmerkmal stellen Zertifizierungen dar. Im Sicherheits- und Qualitätsmanagementbereich wäre bspw. ISO 27001 zu nennen. Im Bereich des Datenschutzes kann auf die Verordnung über die Datenschutzzertifizierung (VDSZ) oder GoodPriv@cy verwiesen werden. Ein Sicherheitsaudit ist jedoch immer nur eine Momentaufnahme und sollte deshalb in regelmässigen Abständen wiederholt werden [25].

6.2 Daten-Back-up. Auf die Cloud sollte man sich nicht blind verlassen. Ein Vorteil besteht sicherlich darin, dass der Cloud-Anbieter automatisch Back-ups erstellt und bei einem Serverausfall sofort auf einen neuen Server wechselt. Ein reibungsloses Weiterarbeiten ist deshalb meist gewährleistet. Das darf aber nicht darüber hinwegtäuschen, dass selbst die Cloud ihre Grenzen hat. Es ist daher empfehlenswert, weiterhin in gewissen Abständen ein eigenes Back-up zu erstellen, das z. B. auf einer externen Festplatte gespeichert wird [26]. Nicht bei jeder Cloud-Lösung ist dies einfach umsetzbar. Da ein Treuhänder im Auftrag von Kunden arbeitet und für die Arbeitsergebnisse eine gesetzliche Aufbewahrungspflicht besteht, ist unbedingt ein Notfallkonzept in Bezug auf die Datenspeicherung auszuarbeiten. Kann bspw. die gesetzliche Aufbewahrungspflicht der Geschäftsbücher [27] nicht mehr erfüllt werden, kann nicht nur ein existenzgefährdender Reputationsschaden entstehen, sondern der Treuhänder kann für den entstandenen Schaden allenfalls haftbar gemacht werden. Fällt der Cloud-Anbieter aus oder fällt er gar in Konkurs, so sind mit einem regelmässigen externen Back-up die (meisten) Daten nicht verloren. Was die Daten anbelangt, so gilt es zu bemerken, dass diese bis heute nicht als Sache gelten und somit nicht einfach herausverlangt werden können. Selbst wenn die Daten herausgegeben werden, dauert es eine gewisse Zeit [28].

«Es ist empfehlenswert, weiterhin in gewissen Abständen ein eigenes Back-up zu erstellen.»

7. DATENAUFBEWAHRUNG

Grundsätzlich können die Belege usw. weiterhin in Papierform bearbeitet werden. Soll durch die Cloud-Lösung gleichzeitig ein ortsungebundenes Arbeiten ermöglicht werden, müssen die Belege digitalisiert werden, da sonst viele Arbeiten nicht ausgeführt werden können. Die gescannten Belege können auch nur für das Arbeiten benutzt werden, während weiterhin die Papierbelege archiviert werden. Wird der Aufwand eines Scannings betrieben, kann eine digitale Archivierung Sinn ergeben, da die Dokumente bereits in digitaler Form vorliegen. Da es sich beim Scanning um einen Medienbruch handelt, gilt es einige rechtliche Stolpersteine zu beachten.

Das Gesetz schreibt vor, dass die Geschäftsbücher und die Buchungsbelege sowie der Geschäftsbericht und der Revisionsbericht während zehn Jahren aufzubewahren sind. Die Geschäftsbücher und die Buchungsbelege können auf Papier, elektronisch oder in vergleichbarer Weise aufbewahrt werden, soweit dadurch die Übereinstimmung mit den zugrunde liegenden Geschäftsvorfällen und Sachverhalten gewährleistet ist und wenn sie jederzeit wieder lesbar gemacht werden können [29]. Eine elektronische Aufbewahrung ist somit aus Buchführungssicht möglich. Wobei digital erhaltene Belege wie bspw. E-Rechnungen gemäss der Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) [30] zwingend elektronisch aufbewahrt werden müssen und somit eine Papierarchivierung nicht möglich ist. Es gilt dabei aber zwischen der Ablage und der Archivie-

rung zu unterscheiden. Die Ablage dient der kurz- und mittelfristigen Aufbewahrung und Verwaltung von Informationen und Dokumenten. Das Ziel ist der schnelle und einfache Zugriff auf die Information. Sinnvollerweise sind Dokumente, die sich in der Ablage befinden, veränderbar. Darum wird die Ablage auch als dynamischer Teil eines *Dokumentenmanagementsystems (DMS)* und als Vorstufe zur Archivierung betrachtet. Veränderungen eines Dokuments müssen aber auch in einem DMS nachvollziehbar sein, um eine spätere Archivierung zu ermöglichen. Das elektronische Archiv als Endablage ist der statische Teil des DMS. Die elektronische Archivierung dient der langfristigen, strukturierten, statischen und unveränderbaren Aufbewahrung elektronischer Informationen (z. B. gescannte Dokumente, Office-Dokumente, Host-Daten, Druckdateien und andere archivwürdige Objekte) [31]. Die genauen Anforderungen sind in der *Geschäftsbücherverordnung (GeBüV)* geregelt. Die Authentizität und die Integrität der elektronisch aufbewahrten Daten müssen bis zum Eintritt der Verjährung prüfbar bleiben [32]. Zur Aufbewahrung zulässige Informationsträger sind unveränderbare Informationsträger wie Papier, Bildträger und unveränderbare Datenträger (z. B. WORM, CD, DVD). Die Verwendung veränderbarer Informationsträger (z. B. Disketten, Festplatten) sind unter folgenden Auflagen nach Art. 9 Abs. 1 GeBüV zulässig:

→ Gewährleistung der Integrität durch technische Verfahren (digitale Signatur); → unverfälschbarer Nachweis des Zeitpunkts der Informationsspeicherung (z. B. durch Zeitstempel); → Einhaltung der Vorschriften über den Einsatz technischer Verfahren; → Festlegung und Dokumentation der Abläufe und Verfahren zu deren Einsatz sowie Aufbewahrung der Hilfsinformationen (Protokolle, Logfiles usw.).

Die Integrität und Lesbarkeit der Informationsträger ist gemäss Art. 10 Abs. 1 GeBüV regelmässig zu überprüfen. Datenüberträge auf neue Informationsträger sind während der Aufbewahrungszeit zulässig und meist auch notwendig, um die Lesbarkeit über die gesamte Aufbewahrungsdauer garantieren zu können [33], weshalb es bei der Auswahl eines Cloud-Anbieters die Möglichkeit der Migration unbedingt zu berücksichtigen gilt.

Neben den Buchführungs- und steuerrechtlichen Aufbewahrungspflichten müssen die elektronischen Dokumente im schlechtesten Fall als Beweismittel verwendet werden können. Dabei kann durch den Medienbruch ein Beweisproblem entstehen, bspw. wenn es auf die Unterschrift auf dem Dokument ankommt. So hat das Bundesgericht in einem aktuellen Fall die Zulässigkeit eines grafologischen Gutachtens anhand einer digitalisierten Kopie verneint. Da das Original nach der Digitalisierung vernichtet wurde, konnte es nicht

mehr als Beweis beigebracht werden [34]. Um dieses Risiko zu vermeiden, sollten Belege, auf denen die Unterschrift oder andere Merkmale des Originaldokuments wesentlich sind, nicht vernichtet, sondern im Original archiviert werden. Falls es sich um Kundenbelege handelt, können diese auch an den Kunden retourniert werden. Soll kein physisches Archiv mehr geführt werden, sollte der Kunde auf das Rechtsrisiko hingewiesen werden [35]. Es bleibt zu hoffen, dass sich für dieses Problem in Zukunft eine Lösung finden wird, um eine vollständige und rechtssichere Digitalisierung von Dokumenten zu ermöglichen.

8. VERANTWORTUNG

Die Verantwortung des Treuhänders gegenüber dem Kunden in Bezug auf die Cloud-Lösung ist abhängig davon, ob der Klient oder der Treuhänder den Vertrag mit dem Cloud-Anbieter eingegangen ist. Schliesst der Kunde einen Vertrag mit dem Cloud-Anbieter, haftet der Treuhänder gegenüber dem Kunden höchstens aufgrund der Schlechterfüllung seiner Treuhanddienstleistung gemäss Art. 398 Abs. 1 und 2 des *Obligationenrechts (OR)* [36]. Leistungsstörungen hat der Kunde somit direkt mit dem Cloud-Anbieter zu lösen. Der Treuhänder trägt keine Verantwortung für das Funktionieren der Software, womit sein Haftungsrisiko vermindert ist.

Schliesst der Treuhänder einen Vertrag direkt mit dem Cloud-Anbieter ab, haftet der Treuhänder einerseits für eine allfällige Schlechterfüllung seiner Treuhanddienstleistung (vgl. Art. 398 Abs. 1 und 2 OR), andererseits trägt er gegenüber dem Kunden das Risiko einer nicht funktionierenden Infrastruktur. Vielfach reduziert der Cloud-Anbieter seine Haftung auf das gesetzliche Minimum, womit ein Regress zwar möglich ist, aber der Folgeschaden beim Kunden wohl meist von der Haftung ausgeschlossen sein wird. Dies gilt wohl selbst dann, wenn der Kunde den Treuhänder zum Beizug eines Cloud-Anbieters ausdrücklich ermächtigt hat (Substitution [37]). Da der Beizug des entsprechenden Cloud-Anbieters überwiegend im Interesse des Treuhänders liegt, würde Letzterer wahrscheinlich nach Art. 101 OR (Cloud-Anbieter als Hilfsperson) haften und nicht nur für eine sorgfältige Auswahl und Instruktion [38].

Da ein Treuhänder erster Ansprechpartner bei Finanz- und Buchhaltungsfragen ist, liegt es zudem nahe, ihn bei der Beschaffung einer neuen Software- oder Cloud-Lösung um Rat zu fragen. Gibt ein Treuhänder eine Empfehlung ab, muss er sich seiner auftragsrechtlichen Sorgfaltspflichten bewusst sein. Fehlt dafür das technische Wissen, sollte auf einen IT-Experten verwiesen oder ein solcher beigezogen werden.

9. FAZIT

Die Digitalisierung eröffnet dem Treuhänder zwar neue und effizientere Arbeitsmöglichkeiten, aber ebenso entstehen neue Risiken, die entsprechend adressiert werden müssen. Möchte ein Treuhänder einen Cloud-Service nutzen, hat er vorgängig die eigenen Bedürfnisse genau zu analysieren, um eine bedürfnisgerechte Auswahl des Cloud-Anbieters treffen zu können. Bei der anschliessenden Vertragsgestaltung ist von elementarer Bedeutung, dass die zu erbringenden Leistungen im Vertrag detailliert und präzise umschrieben werden. Wird gleichzeitig auf eine digitale Datenablage und Archivierung umgestellt, ist eine rechtssichere Aufbewahrung sicherzustellen. ■

Anmerkungen: 1) http://www.kmu-businessworld.ch/de/management/die-zukunft-liegt-der-cloud. **2)** Bundesamt für Sicherheit in der Informatik, Cloud Computing, unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/CloudComputing-Grundlagen.html, aufgerufen am 17.10.2016. **3)** Sury Ursula/Gogniat Yves, Umzug einer Kanzlei in die Cloud, in: Anwaltsrevue de l'avocat 5/2015, S. 201. **4)** Vgl. Hoffmann Rauno, Cloud Computing – Services und deren datenschutzrechtliche Voraussetzungen, in: Der Schweizer Treuhänder 2012/6–7, S. 465 ff. **5)** Straub Wolfgang, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 2014, S. 905 ff. **6)** Mathys Roland, 5/6.3 IT-Outsourcing-Vertrag, in: WEGA Verlag AG, Informatikrecht in der Praxis, 2008, 5/6.3.3, S. 1. **7)** Fröhlich-Bleuler, Softwareverträge, Bern 2014, Rz. 2554. **8)** Die Verfügbarkeit wird häufig als Prozentsatz der vereinbarten Nutzungszeit (z. B. an Wochentagen von 7.00 bis 18.00 Uhr), bezogen auf einen definierten Zeitraum (Woche, Monat, Jahr), festgelegt. **9)** Sury, Informatikrecht, S. 63. **10)** Eine Lizenz für zehn Concurrent-User darf z. B. von mehr als zehn Usern genutzt werden, allerdings können zu jedem Zeitpunkt nur maximal zehn User gleichzeitig darauf zugreifen. **11)** Eine Software mit einer Lizenz für z. B. zehn Named-User kann ausschliesslich von den maximal zehn registrierten, eingetragenen Usern genutzt werden. **12)** Vgl. Lanz Philipp/Bandle Olivier, Anforderungen an Cloud-Lösungen für den Treuhandbereich, mit einem Fragekatalog zu Cloud-Lösungen für Treuhänder, in: Expert Focus 2016/1–2, S. 21; Straub Wolfgang, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 2014, S. 907. **13)** Gordon Clara-Ann, Cross-Border Outsourcing und Datenschutz, Seminar vom 28. September 2016 zum Thema Cross-Border Outsourcing – Rechtsfragen und Lösungen, Vertragliche und andere rechtliche Massnahmen zur Steuerung von grenzübergreifenden Outsourcing Projekten, Folie 17 f. **14)** Sury Ursula/Gogniat Yves, Umzug einer Kanzlei in die Cloud, in: Anwaltsrevue de l'avocat 5/2015, S. 203. **15)** Vgl. EDÖB, Leitfaden für die Bearbeitung von Personendaten im privaten Bereich, August 2009, S. 4. **16)** Expertsuisse, Standes- und Berufsregeln, 2007, Ziffer IV. **17)** Vgl. Schwaninger David/Lattmann Stephanie, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013, S. 3. **18)** Hoffmann Rauno, Cloud Computing, in: Der Schweizer Treuhänder, 2012/6–7, S. 466. **19)** Pfaff Dieter/Sury Ursula/Gogniat Yves/Jaquet Roger, Schweizer Compliance Standard, E-Rechnung in der Schweiz, Zürich 2016, S. 44, abrufbar unter https://veb.ch/fileadmin/documents/publikationen/veb_ComplianceStandard_E_Rechnung_2016.pdf. **20)** http://www.edoeb.admin.ch/datenschutz/00626/00753/00969/index.html?lang=de. **21)** Als aktuelles Beispiel kann hier auf einen Fall in den USA verwiesen werden: Winfield Nick/Kang Cecilia, Microsoft Wins Appeal on Overseas Data Searches, The New York Times, http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html?_r=0, aufgerufen am 17.10.2016. **22)** Art. 10 Abs. 4 ElDI-V. **23)** Vgl. von Bhicknapahari Sikander, VEB Praxiskommentar, N 36 ff. zu Art. 958 f. OR. **24)** Art. 7 und insb. Art. 10a Abs. 2 DSG in Bezug auf das Outsourcing. **25)** Vgl. Sury Ursula/Gogniat Yves, Umzug einer Kanzlei in die Cloud, Anwaltsrevue de l'avocat 5/2015, S. 204. **26)** Vgl. Sury Ursula/Gogniat Yves, Umzug einer Kanzlei in die Cloud, Anwaltsrevue de l'avocat 5/2015, S. 204 f. **27)** Art. 958 f OR. **28)** Vgl. Wyss Ralph, IT in der Insolvenz, in: Europa Institut an der Universität Zürich, Sanierung und Insolvenz von Unternehmen IV, Zürich/Basel/Genf 2014, S. 66 ff. **29)** Art. 958 OR. **30)** Art. 10 ElDI-V. **31)** Pfaff Dieter/Sury Ursula/Gogniat Yves/Jaquet Roger, Schweizer Compliance Standard, E-Rechnung in der Schweiz, Zürich 2016, S. 29. **32)** Vgl. MWST-Info, 1.6. Aufbewahrung, 16.1. Aufbewahrungsart, https://www.gate.estv.admin.ch/mwst-webpublikationen/public/pages/taxInfos/cipherDisplay.xhtml?publicationId=1002536&componentId=1002571&cipherKeyDate=01.01.2013&lang=de&redirect=true&rmSel=true&&&winid=597750, aufgerufen am 17.10.2016. **33)** Pfaff Dieter/Sury Ursula/Gogniat Yves/Jaquet Roger, Schweizer Compliance Standard, E-Rechnung in der Schweiz, Zürich 2016, S 14. **34)** BGer Urteil 9C_634/2014 vom 31. August 2015. **35)** Fässler Lukas, Durchklick: Elektronische Aktenführung – Beweisführung mit eingescannten Dokumenten, in: Anwaltsrevue 09/2014, S. 385. **36)** Weber Rolf H., BSK, Basel 2011 N 22 zu Art. 398 OR; Fellmann Walter, BK, Bern 1992, N 486 zu Art. 398 OR. **37)** Art. 399 OR. **38)** Vgl. Art. 399 Abs. 2 OR.