UMZUG EINER KANZLEI IN DIE CLOUD

URSULA SURY
Rechtsanwältin bei Die Advokatur Sury und Professorin an der Hochschule Luzern

YVES GOGNIAT
Rechtsanwalt bei Die Advokatur Sury

Stichworte: Kanzlei IT, Cloud Computing, Cloud, Anwaltsrecht, Datenschutz, Archivierung

Der vorliegende Beitrag soll dem Leser einen Überblick über die rechtlichen Fragen und die wirtschaftlichen Überlegungen beim Umzug einer kleineren Kanzlei in die Cloud geben. Daneben informiert der Beitrag über die praktischen Erfahrungen und Überlegungen, die sich die Autoren bei der eigenen Umstellung gemacht haben.

I. Ausgangslage

1. Die IT in einer Kanzlei

Die IT ist inzwischen auch für Anwälte zu einem unverzichtbaren Arbeitsmittel geworden. Die Kommunikation mit den Klienten erfolgt zum überwiegenden Teil via E-Mail. Mittlerweile ist es völlig selbstverständlich, die ganze Korrespondenz, Rechtschriften, Aktennotizen etc. auf dem PC zu verfassen, sodass wir nicht einmal mehr einen Gedanken daran verschwenden – zumindest solange alles einwandfrei funktioniert! Ohne funktionierende IT steht eine Kanzlei praktisch still. Dies ist ein Albtraum für jeden Anwalt, zu dessen wichtigsten Pflichten die Einhaltung von Fristen und Terminen gehört. Es will daher immer wohl überlegt sein, wem die IT anvertraut wird, egal ob man sich für eine lokale oder externe bzw. Cloud-Lösung entscheidet. Die Verfügbarkeit und Sicherheit muss jederzeit sichergestellt sein. Die gute Nachricht ist, dass die Kanzlei-IT nicht besonders komplex ist. Die meisten Kanzleien nutzen nur Standardprodukte, was den Aufwand in Grenzen hält und gerade eine Cloud-Lösung nicht besonders aufwendig macht.

2. Die Cloud

Was ist überhaupt unter dem Begriff Cloud zu verstehen. Die Cloud 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 erfolgen 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 anderen Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.[1] D. h., bei Cloud Computing wird die Informatik nicht mehr selbst bereitgestellt und betrieben, sondern als Dienst bedarfsgerecht gemietet. Die Soft- und Hardware befinden sich nicht mehr im 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. Im vernebelten Umfeld der Cloud ist es für den Outsourcer oft schwer, festzustellen, wer genau sein Vertragspartner ist.[2]

Für einen outsourcenden Anwalt ist es wichtig, dass er alle involvierten Dienstleister kennt. Durch sein Berufsgeheimnis hat er besondere Sorgfaltspflichten wahrzunehmen und muss sicherstellen, dass die Hilfspersonen sich ebenfalls daran halten. Aus diesem Grund haben wir uns für einen Cloud-Dienstleister entschieden, der alles aus einer Hand bietet. D. h., der Anbieter betreibt nicht nur das Rechenzentrum, sondern er richtet auch die virtuellen Arbeitsplätze ein und betreibt den E-Mail-Server. Ausserdem braucht es noch einen Lieferanten für die lokalen Geräte und natürlich den Provider für Internet und Telefon. Nachfolgend wird von dieser Konstellation ausgegangen und nicht auf komplexere Verhältnisse eingegangen.

II. Wirtschaftliche Aspekte

1. IT-Kosten

In dieser Beziehung unterscheidet sich eine Anwaltskanzlei nicht von anderen Unternehmen, die IT-Infrastruktur muss in regelmässigen Abständen wieder auf den neusten Stand gebracht werden, um ein effizientes und sicheres Arbeiten zu ermöglichen. Ausserdem handelt es sich um

1 Bundesamt für Sicherheit in der Informatik, Cloud Computing, unter https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html aufgerufen am 22. 4. 2015.
2 Vgl. TSCHOL DANIELA, Cloud Computing, in IT business 1/2011, S. 46.

Kosten, die keinen direkt sichtbaren Mehrwert bieten. Ob mit dem neusten Windows-Betriebssystem oder mit einer älteren Version gearbeitet wird, macht für die meisten Anwender in der Praxis keinen Unterschied. Trotzdem zwingt einen das Umfeld alle paar Jahre, die IT auf den neusten Stand zu bringen. Viele ersetzen die IT deshalb erst, wenn es nicht mehr anders geht, und vernachlässigen dadurch die Sicherheit. So liefen 13,6% aller Windows-Rechner im November 2014 auf Windows XP, obwohl der Support eingestellt wurde.[3]

Mit zehn Arbeitsplätzen ist unsere Kanzlei nicht sehr gross, nichtsdestotrotz verursacht ein Ersetzen aller Arbeitsplätze grössere Kosten. Der Nachteil bei diesem zyklischen Modell: Die Kosten fallen alle paar Jahre als Gesamtblock an. Dies kann unerwünscht sein, obwohl natürlich die Arbeitsplätze fortlaufend ersetzt werden können. Allerdings sind die Installation und das Einrichten eines einzelnen Arbeitsplatzes teurer als eine Gesamterneuerung, da die Einrichtung eines einzelnen Arbeitsplatzes ineffizient ist.

Bei der bis anhin bestehenden Inhouse-Lösung hat die Administrationsmitarbeiterin jeweils den Arbeitsplatz für einen neuen Mitarbeiter eingerichtet. Dies dauerte fast einen halben Arbeitstag. In dieser Zeit konnte sie nicht anderweitig eingesetzt werden. Dies zeigt, dass auch verdeckte Kosten nicht vernachlässigt werden dürfen. Zudem hat sich beim externen Support gezeigt, dass es gerade für eine kleine Kanzlei schwer ist, einen guten IT-Support zu finden, der ein vernünftiges Preis-Leistungs-Verhältnis bietet und in der Lage ist, alle Aspekte – von den Sicherheitsthemen bis hin zum Support der kleinen Probleme – zeitnah und in guter Qualität abzudecken.

Alle diese Punkte sind in die Entscheidungsfindung für den Umstieg mit eingeflossen. Trotzdem ist ein direkter Vergleich der Kosten nur schwer möglich. Günstiger wird die IT durch den Wechsel gesamtkostenmässig wahrscheinlich nicht, dies wird sich erst in einer Nachkalkulation zeigen. Der Vergleich wird aber wegen der unterschiedlichen Services schwierig sein. Den Ausschlag für einen Wechsel haben schlussendlich andere Punkte gegeben. Jeder Mitarbeiter hat nun seinen eigenen virtuellen Arbeitsplatz in der Cloud. Das Aufsetzen eines neuen Arbeitsplatzes geht schneller und wird direkt vom Anbieter erledigt. Durch das virtuelle Arbeiten ist nun ein Desk Sharing möglich. Theoretisch kann nun jeder Mitarbeiter von jedem PC in der Kanzlei auf seine persönliche Umgebung zugreifen und arbeiten. Dies bringt vor allem Vorteile für unsere Teilzeitarbeitskräfte. Durch den Anschluss an den Cloud-Anbieter kann von dessen Skaleneffekten profitiert werden. Ständige Sicherheits- und Softwareupdates im gleichen Ausmass wären bei einer lokalen Lösung wohl kaum möglich. Im Gegensatz zu einem kleinen IT-Unternehmen, welches normalerweise kleine Kanzleien für lokale Lösungen betreut, ist es für einen Cloud-Anbieter möglich, für alle Bereiche spezialisierte Mitarbeiter einzustellen. So zum Beispiel einen Sicherheitsspezialisten oder einen Windows-Supportmitarbeiter. Zusätzlich bietet unser Anbieter als One-Stop-Shop noch diverse Zusatzleistungen wie Back-up, automatische Verschlüsselung der E-Mail, sicheres externes Arbeiten etc. Der Verwaltungsaufwand der IT lässt sich dadurch wesentlich reduzieren und schafft freie Ressourcen für die Betreuung der Klienten. Der Nachteil einer Cloud-Lösung sind die kontinuierlichen Kosten, diese sind dafür besser planbar.

2. Arbeitsweise

A) Externe Einflüsse

Wir teilen die Ansicht von Straub, dass für die Mandatsvergabe die IT-Ausstattung einer Kanzlei ebenso wenig entscheidend sein dürfte wie eine gute Lage oder eine elegante Büroeinrichtung. Potenzielle Klienten fragen praktisch nie danach, welche IT-Systeme im Einsatz sind. Allerdings ist eine leistungsfähige Infrastruktur Voraussetzung für die Abwicklung bestimmter Mandate und wird von den Klienten einfach erwartet. Die IT kann aber auch dabei helfen, effizienter zu arbeiten und den Klienten einen besseren Service zu bieten.[4] Gerade in unserer Kanzlei kommt das externe Arbeiten relativ häufig vor und wird von Unternehmen immer häufiger verlangt. Bspw. ist für ein Datenschutzaudit die Anwesenheit vor Ort notwendig. Die Cloud-Anwendung erlaubt es uns, kostengünstig einen externen Zugriff einzurichten. Gewiss kann in den meisten Fällen ohne einen solchen beim Kunden gearbeitet werden. Er erlaubt einem aber ein effizienteres Arbeiten. Ausser auf das entsprechende Klientendossier kann ebenso auf das kanzleiinterne Wissensmanagement zugegriffen werden. Natürlich braucht es nicht zwingend eine Cloud-Lösung, um einen externen Zugang einzurichten. Eine sichere und zuverlässige Lösung via lokalen Server ist für eine kleine Kanzlei aber nicht günstig umsetzbar.

Der Trend vom physischen Arbeitsplatz hin zum mobilen Arbeiten wird sich in Zukunft noch verstärken. Die Anwaltsbranche ist noch skeptisch und zurückhaltend, trotzdem wird sie sich dieser Entwicklung nicht entziehen können.

B) Interne Einflüsse

Eine Veränderung des Arbeitens wird nicht nur von den Klienten verlangt. Auch Mitarbeiter fordern die Möglichkeiten, flexibler zu arbeiten. Wie eine Umfrage unter jungen Anwälten in deutschen Grosskanzleien gezeigt hat, hat die Generation Y heute andere Ansprüche an einen Arbeitgeber. 96 Prozent der Befragten äusserten etwa, ihnen sei Work-Life-Balance «sehr wichtig». 83 Prozent wollten niedrigere Löhne akzeptieren, wenn damit ein verringertes Arbeitsaufkommen einherginge. Und 96 Prozent gaben an, dass der Wunsch, weniger zu arbeiten,

3 MATTHIAS BRANDT, XP stürzt auch im November weiter ab, http://de.statista.com/infografik/798/weltweite-marktanteile-ausgewaehlter-windows-betriebssysteme/ aufgerufen am 21. 4. 2015.

4 WOLFGANG STRAUB, Durchblick: Was bringt die IT in der Anwaltskanzlei? – Teil 2, in Anwaltsrevue 1/2013, S. 21.

durchaus nicht den Rückschluss auf fehlende Motivation erlaube. Nichtjuristen mag das selbstverständlich und kaum erwähnenswert erscheinen – doch in der arbeitsversessenen Welt der Grosskanzleien klingen solche Präferenzen direkt umstürzlerisch.[5] Neben den Juristen gilt es an das Administrationspersonal zu denken, da dieses am stärksten von der IT betroffen ist. Viele davon arbeiten bereits heute in Teilzeit.

Auch hier bietet eine Cloud-Lösung Möglichkeiten, diesen Trend kostengünstig aufzufangen. Durch das Arbeiten auf virtuellen Arbeitsplätzen in der Cloud sind Desk Sharing, Home Office und mobiles Arbeiten möglich. Teilzeitmitarbeiter können jetzt dort arbeiten, wo gerade ein Arbeitsplatz frei ist, und sind nochmals flexibler in der zeitlichen Organisation. Bei guter Planung kann dadurch sogar Bürofläche eingespart werden, da die einzelnen Arbeitsplätze besser ausgelastet werden.

III. Rechtliche Aspekte

1. Grundlagen

In diesem Kurzüberblick der rechtlichen Aspekte wird der Fokus auf das Berufsgeheimnis und den Datenschutz gelegt. Eine umfassende Darstellung würde den Rahmen dieses Artikels sprengen. Natürlich dürfen daneben die handelsrechtlichen und steuerrechtlichen Themen nicht vergessen werden. Vor allem im Kontext der Aufbewahrungspflicht bzw. bei der Archivierung.

2. Berufsgeheimnis

Die erste rechtliche Frage die sich ein Anwalt beim Thema Cloud stellt, ist sicherlich die Frage nach der Einhaltung des Berufsgeheimnisses. Gemäss Art. 13 BGFA unterstehen die Anwältinnen und Anwälte zeitlich unbegrenzt und gegenüber jedermann dem Berufsgeheimnis über alles, was ihnen infolge ihres Berufes von ihrer Klientschaft anvertraut worden ist. Die Tätigkeit im Rahmen des Anwaltsmonopols ist zweifellos geschützt. So umfasst das Berufsgeheimnis sämtliche dem Anwalt anvertrauten Tatsachen und Dokumente, die einen gewissen Bezug zur Ausübung des Anwaltsberufs haben. Gemäss der Rechtsprechung des Bundesgerichts können sich Anwälte, die für eine Klientschaft andere Tätigkeiten als spezifische Anwaltstätigkeiten ausüben, demgegenüber nicht auf das Anwaltsgeheimnis berufen. Wirtschaftliche Tätigkeiten von Anwälten, beispielsweise die Verwaltung von Gesellschaften und Vermögen, die Betreuung von Fonds, also Tätigkeiten, die auch von Vermögensverwaltern, Treuhändern und Bankiers ausgeübt werden können, werden vom Anwaltsgeheimnis nicht geschützt.[6] Die Nutzung einer Cloud ist gerade für eine kleinere Kanzlei nur sinnvoll, wenn sie mit allen Daten in die Cloud wandert. Eine Trennung von Daten, die dem Anwaltsgeheimnis unterliegen, und anderen Daten scheint nicht zweckmässig, nicht praktikabel und gar nicht notwendig, da der Anbieter sowieso mit allen Daten in Berührung kommt. Das Berufsgeheimnis ist daher auch in der Cloud zu wahren. Relevant in Bezug auf die Cloud ist, dass ein Anwalt auch für die Einhaltung des Berufsgeheimnisses der Hilfspersonen verantwortlich ist. Dies ergibt sich sowohl aus Art. 13 Abs. 2 BGFA als auch aus Art. 101 OR. Kaum ein Anwalt wird seine gesamte IT selbstständig betreuen, er zieht also bereits heute Hilfspersonen hinzu. Natürlich besteht bei einer Inhouse-Lösung immer die Möglichkeit den IT-Leuten auf die Finger zu schauen, wobei das heute vielfach nur noch begrenzt möglich ist, da viele mit Fernwartungstools arbeiten. Es hat also vor allem einen psychologischen Effekt, wenn ich den Server im eigenen Büro anschauen kann. Ich kann den IT-Leuten zwar zuschauen, aber weiss als Durchschnittsnutzer eigentlich trotzdem nicht, was gemacht wird. Selbst bei einer Inhouse-Lösung muss ich meinen IT-Support zur Verschwiegenheit verpflichten. Im Prinzip ändert sich also zu einer Cloud-Anwendung nichts bei der Hilfspersonenhaftung, sofern sich der Cloud-Anbieter in der Schweiz befindet. Bei beiden Varianten muss das IT-Unternehmen in die Pflicht genommen und sicherstellt werden, dass dieses auch seine Mitarbeiter zur Diskretion anhält.

Ein Verstoss gegen das Berufsgeheimnis wird nach Art. 321 StGB geahndet. Hilfspersonen fallen auch unter Art. 321 StGB. Ein Cloud-Anbieter gilt als Hilfsperson im Sinne aller der genannten Bestimmungen. Es empfiehlt sich, vertraglich festzuhalten, dass alle Daten, welche die Kanzlei dem Anbieter übermittelt, als vertraulich (oder geheim) gelten und nicht ohne (schriftliche) Zustimmung an Dritte weitergegeben werden dürfen. Zudem sollte die Unterzeichnung des Anwaltsgeheimnisses von den Mitarbeitern verlangt werden, die Zugriff auf die Daten erhalten könnten.

3. Datenschutzrecht

Neben den anwaltlichen Sorgfaltspflichten gilt es, das Datenschutzrecht zu beachten. Sobald eine private Person innerhalb einer Cloud Daten von natürlichen oder juristischen Personen bearbeitet, ist das eidgenössische Datenschutzgesetz anwendbar. In Klientendossiers werden immer Personendaten bearbeitet. Gemäss Art. 4 und Art. 5 DSG müssen bei jeder Datenbearbeitung die Grundsätze des DSG respektiert werden. Personendaten müssen rechtmässig erhoben werden, dies sollte in einer Kanzlei eigentlich unproblematisch sein. Die Personendaten müssen nach Treu und Glauben und nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[7] In der Kanzlei ist die Einhaltung dieser Grundsätze unproblematisch und kann leicht kontrolliert werden. Das Risiko eines Fehlverhaltens ist gering, da die

5 CONSTANTIN BARON VAN LIJNDEN, Aussterbende Art Arbeitstier, http://www.spiegel.de/karriere/berufsstart/work-life-balance-extreme-arbeitszeiten-von-juristen-in-grosskanzleien-a-827265.html aufgerufen am 21. 4. 2015.

6 Botschaft zum BGFA vom 28.4., BBl 1999, S. 6055.

7 Vgl. EDÖB, Leitfaden für die Bearbeitung von Personendaten im privaten Bereich, August 2009, S. 4.

Mitarbeiter bereits aufgrund des Anwaltsgeheimnisses sensibilisiert auf den Umgang mit Daten sind. Die Personendaten befinden sich nun aber in der Cloud, der Cloud-Anbieter muss deshalb auch in die Pflicht genommen werden. Das Speichern von Personendaten in einer Cloud, ermöglicht eine sogenannte Datenbearbeitung durch Dritte dar.

Das Auslagern von Daten in die Cloud ist nach Art. 10a DSG grundsätzlich zulässig, und zwar auch ohne Einwilligung der betroffenen Personen. Die Daten dürfen aber nur bearbeitet werden, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht die Bearbeitung durch einen Dritten verbietet, und nur so, wie es die Kanzlei selber dürfte. Es muss ausserdem sichergestellt werden, dass der Cloud-Anbieter die notwendigen Voraussetzungen für eine datenschutzkonforme Datenbearbeitung erfüllt und insbesondere die Datensicherheit gewährleistet. Eine sorgfältige Auswahl des Anbieters ist deshalb zwingend. Eine vorgängige Prüfung des Anbieters auf die Einhaltung des Datenschutzes ist 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.[8] Im Aktivbetrieb gilt es zudem, den Anbieter zu überwachen, sonst hilft auch der beste Vertrag nicht viel. Es darf nicht vergessen werden, der Cloud-Anbieter ist auch hier nur Hilfsperson, und die Haftung kann nicht auf diesen überbunden werden.

IV. Sicherheit

1. Anbieter Cloud-Lösung

A) Sicherheitsstruktur

Wie oben ausgeführt muss Sicherheit in Bezug auf den Datenschutz bestehen. Dies kann vertraglich geregelt und durch Überprüfen der Reglemente und Prozesse des Cloud-Anbieters sichergestellt werden. Dieser Aufgabe sollte ein Anwalt gewachsen sein. Eine technische Sicherheitsprüfung dagegen ist normalerweise zu komplex für einen Anwalt. In unserem Fall haben wir unseren Cloud-Anbieter durch einen Informatikspezialisten prüfen lassen, um sicherzugehen, dass die notwendigen Sicherheitsmassnahmen (Firewall, Antivirus, Verschlüsseln) vorhanden und auf dem neusten Stand sind. Zudem konnte er die fachliche Kompetenz der Mitarbeiter besser einschätzen. Ein solches Sicherheitsaudit ist jedoch nur eine Momentaufnahme und sollte deshalb in regelmässigen Abständen wiederholt werden. Ein weiteres Qualitätsmerkmal für einen fähigen Anbieter stellen Zertifizierungen dar. Im Sicherheits- und Qualitätsmanagementbereich wären da bspw. die ISO 9001 Norm oder die ISO 27001 Norm zu nennen. Im Bereich des Datenschutzes kann auf die Datenschutzzertifizierung VDSZ verwiesen werden.

Beim Server selbst haben wir uns für einen Private Server und nicht für einen Shared Server entschieden. Ein Zugriff eines anderen Kunden auf unseren Server ist technisch nicht möglich.

Die Abhängigkeit vom Cloud-Anbieter kann durch vorsorgliche Massnahmen reduziert, aber leider nicht ganz aufgefangen werden. Ausserdem bekommt der Provider der Internetleitung einen höheren Stellenwert. Für die Nutzung der Cloud ist in den meisten Fällen eine Erhöhung der Bandbreite notwendig.[9] Daneben sollte beim Provider noch die zugesicherte Responsetime überprüft werden, evtl. lohnt es sich, diese durch den Abschluss eines Zusatzvertrages zu erhöhen, um im Falle einer Störung eine schnelle Reaktionszeit zu gewährleisten. Läuft die Verbindung nur langsam oder gar nicht, bringt der beste Cloud-Anbieter nichts. Für eine sichere Internetverbindung ohne Unterbrechung können zwei Internetzugänge parallel installiert werden. Damit wird das Risiko eines Totalausfalls stark reduziert.

B) Standort

Wo sich der Anbieter in der Schweiz befindet, ist im Prinzip egal, wichtig war uns aber, dass der Anbieter seine Rechenzentren in der Schweiz betreibt und es sich um eine Schweizer Firma handelt. Dadurch kann ausgeschlossen werden, dass eine ausländische Behörde plötzlich über den Cloud-Anbieter auf unsere Klientendaten greifen könnte.[10] Was zu einer Verletzung des Anwaltsgeheimnisses führen könnte und natürlich zu einem nicht absehbaren Reputationsschaden.

C) Notfallkonzept

Blind auf die Cloud kann man sich auch nicht verlassen. Ein Vorteil ist sicherlich, dass der Cloud-Anbieter automatisch Back-ups erstellt und bei einem Serverausfall sofort auf einen neuen Server wechselt. Ein reibungsloses Weiterarbeiten ist deshalb gewährleistet. Ausserdem können leichter einzelne Dokumente wiederhergestellt werden. Das darf aber nicht darüber hinwegtäuschen, dass selbst die Cloud ihre Grenzen hat. Es ist daher empfehlenswert, weiterhin zumindest in gewissen Abständen ein Back-up zu erstellen, welches z. B. auf einer externen Festplatte gespeichert wird. Unser Anbieter bietet einen Back-up-Service an und speichert die gesamten Daten in den gewünschten Zeitabständen auf einem externen Datenspeicher. In unserem Fall erhalten wir diese halbjährlich auf einer Festplatte. Es wäre aber ebenso möglich, die Daten auf einem anderen externen Rechner spiegeln zu lassen. Besteht jedoch plötzlich das Risiko eines Ausfalls, kann natürlich öfter ein Back-up verlangt werden. Zusätzlich ist es ein Einfaches ein Inventar mit den wichtigsten Programmen zu führen, die im täglichen Gebrauch sind.

8 Vgl. DAVID SCHWANINGER/STEPHANIE S. LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke in Jusletter 11. 3. 2013.

9 Mindestens 100 kBit/User werden benötigt.

10 Als aktuelles Beispiel kann hier auf einen Fall in den USA verwiesen werden: Microsoft's data sovereignty battle: a disaster or triumph in the making, unter http://www.pcpro.co.uk/cloud-computing/1000629/microsofts-data-sovereignty-battle-a-disaster-or-triumph-in-the-making aufgerufen am 22. 4. 2015.

Fällt der Cloud-Anbieter aus oder fällt er gar in Konkurs, so können die wichtigsten Programme schnell wieder lokal installiert werden, und falls kein Zugriff mehr auf die Daten besteht, kann zumindest mit dem Back-up der Betrieb aufrechterhalten werden.

2. Arbeiten in der Kanzlei

Um einen sicheren Zugang zu gewährleisten, wird mit einer fixen IP-Adresse gearbeitet. Ein Zugriff auf den virtuellen Arbeitsplatz von einer anderen IP-Adresse ist ohne spezielle Authentifizierung nicht möglich. In der Kanzlei selbst merkt man eigentlich nicht viel von der Umstellung. Erst nach dem Hochfahren und Einloggen am lokalen PC, wird auf den virtuellen Arbeitsplatz gewechselt. Dieser ist wiederum mit einem Passwort geschützt. Der virtuelle Arbeitsplatz läuft danach unabhängig vom lokalen Gerät und die Arbeitsoberfläche sieht wieder genau gleich aus. Dies erhöht die Sicherheit zusätzlich, da ein lokales Einloggen noch keinen Zugriff auf die Kanzleidaten ermöglicht. Wie stark ein Austausch zwischen lokal und virtuell noch möglich sein soll, muss jede Kanzlei für sich selbst bestimmen. Es kann bspw. zugelassen oder verhindert werden, dass ein direktes Abspeichern vom virtuellen Arbeitsplatz auf einen USB-Stick möglich ist. Alternativ könnten auch nur noch Thin Clients verwendet werden. Diese Geräte funktionieren mit weniger Hardware und Rechenleistung, sie stellen nur noch eine Benutzerschnittstelle her und funktionieren nicht mehr als normale Desktop-Geräte.

3. Mobiles Arbeiten

Das mobile Arbeiten wird durch die Cloud-Lösung sicherer und einfacher. Eine schnelle Internetverbindung ist aber Grundvoraussetzung dafür, was heute kein grosses Problem mehr darstellt. Bei einem Verlust oder Diebstahl des mobilen Geräts, kann nicht auf die Daten zugegriffen werden, da nicht mehr lokal gearbeitet wird. Natürlich gilt das nur, wenn keine Daten lokal auf dem Gerät gespeichert werden. Dies ist natürlich den Mitarbeitern mitzuteilen und in einem Reglement festzuhalten.

Im Gegensatz zum Anmelden im Büro, braucht es für das mobile Arbeiten eine spezielle Sicherheitsprüfung. Das Abfragen von Benutzernamen und Passwort reicht dafür nicht aus. Egal ob nun auf eine Cloud zugegriffen oder sonst eine sichere VPN-Verbindung hergestellt wird, in den letzten Jahren hat sich dafür der Einsatz von digitalen Signaturen durchgesetzt, die durch ein separates Stück Hardware erzeugt werden. Eine etwas umständliche Methode ist dabei die Verwendung einer Chipkarte, da ein Lesegerät eingebaut werden muss. Eine einfachere Methode ist der Gebrauch eines Token, der via USB Port genutzt wird. Alternativ können Einmalpasswörter, wie man sie aus dem E-Banking kennt, eingesetzt werden oder auch ein Softtoken, dabei wird das Einmalpasswort bspw. an eine Mobiltelefonnummer per SMS gesandt.[11] Die beiden letzten eignen sich daher für Geräte die keinen USB Port haben. Ausserdem gibt es für mobile Geräte auch APPs die genutzt werden können. Dabei kann sowohl geschützt auf Daten oder Mails zugegriffen werden. Solche Apps erfordern jeweils nochmals ein zusätzliches Passwort. Für eine kleine Kanzlei ist ein solch sicheres System für einen mobilen Zugriff mit einer lokalen Lösung kaum kostengünstig umsetzbar, was aber nicht heisst, dass ein mobiles Arbeiten ohne Cloud nicht möglich wäre, es macht die Technik u. E. einfach leichter einsetzbar für kleine Kanzleien.

V. Digitalisierung und Archivierung

1. Digitales Arbeiten

Das papierlose Arbeiten ist gerade für Anwälte bis heute nur begrenzt möglich. Obwohl sich in den letzten Jahren einiges getan hat. Mittlerweile sind einige juristische Publikationen digital erhältlich. Ebenso ist die elektronische Eingabe bei Gerichten mit der neuen Zivilprozess- und Strafprozessordnung möglich, wenn sich auch die Freude über die elektronische Einreichung bei einigen Gerichten etwas in Grenzen hält.[12] Wie weit die Digitalisierung gehen soll, bleibt weiterhin vor allem eine persönliche Präferenz. Je nach Arbeitsstil wird jedes E-Mail ausgedruckt und in einem physischen Dossier abgelegt. Das andere Extrem ist, dass möglichst gar nichts mehr ausdruckt und nur noch digital gearbeitet wird. Ein digitales Arbeiten ist sicherlich schon alleine je nach Tätigkeitsgebiet und Klientenstamm zu aufwendig, weil die meisten Unterlagen immer noch in Papierform übermittelt werden. Wird der Gedanke der Unabhängigkeit des Arbeitsplatzes, wie oben bereits ausgeführt, konsequent zu Ende gedacht, ist die Verwendung eines digitalen Klientendossiers zwingend. Am Ende waren es aber verschiedene Gründe die den Ausschlag gaben, die Dossiers nur noch elektronisch zu führen. Neben der Reduktion der physischen Abhängigkeit waren hier persönliche Präferenzen mit ausschlaggebend.

Bei der Arbeit mit digitalen Dossiers gibt es einiges zu beachten, um weiterhin seinen Sorgfaltspflichten als Anwalt und den Pflichten nach Auftragsrecht nachzukommen.

Durch die Einführung der neuen Bestimmungen des Obligationenrechts über die kaufmännische Buchführung sowie die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV) folgt der Gesetzgeber im Bereich der Buchführung und Archivierung der elektronischen Entwicklung. In der Praxis gab es längst vor dem Inkrafttreten der neuen Bestimmungen Unternehmen, welche ihre Bücher und Daten elektronisch geführt bzw. archiviert haben. Aufgrund der neuen Bestimmungen drängt sich nun eine Überprüfung der bestehenden Archivierungsprozesse auf. Im Verlaufe der Migration des

11 Vgl. DAVID ROSENTAHL, IT-Sicherheit in der Anwaltskanzlei – Teil 2 in Anwaltsrevue, 9/2006.

12 Vgl. Berner Zeitung online, Gerichte sträuben sich gegen die Online-Justiz, http://www.bernerzeitung.ch/schweiz/standard/Gerichte-straeuben-sich-gegen-die-OnlineJustiz/story/22290166 aufgerufen am 22. 4. 2015.

Cloud-Systems war es daher notwendig, die gesetzlichen Anforderungen im Blick zu behalten und Zertifizierungen seitens des Cloud-Anbieters zu verlangen, um die Einhaltung der gesetzlichen Vorschriften zu garantieren, da ansonsten den entsprechenden Unterlagen allenfalls nur eine geringe Beweiskraft zukommt. Für einen Anwalt, der mit einem elektronischen Dossier arbeitet, ist es essenziell, dass die Beweiskraft der erhaltenen Unterlagen jederzeit gewährleistet ist. Kommt ein neues Dokument durch die (digitale) Kanzleitür, muss es in einem unveränderbaren Dateiformat abgespeichert werden, um die Beweiskraft weiterhin garantieren zu können. Dafür gibt es verschiedene technische Möglichkeiten, eine davon ist, alle Dokumente als PDF/A abzuspeichern.

2. Archivierung

Die digitale Archivierung hängt nicht direkt von der Nutzung einer Cloud-Lösung ab, der Umstieg auf eine solche hat aber den Entscheid dafür mit beeinflusst. Die Weiterführung eines physischen Dossiers wäre auch eine Option gewesen. Genauso wäre eine digitale Archivierung mit einem lokalen Server möglich gewesen. Da wir uns für ein digitales Dossier entschieden haben, ist die digitale Archivierung aber nur die logische Folge.

Beim Einstieg in die Cloud liegt die Verantwortung für die Entwicklung einer Archivierungsstrategie bei der Kanzleiführung. Hierbei darf die Archivierung nicht isoliert betrachtet werden, sondern muss in die bestehenden Geschäfts- und Rechnungswesensprozesse integriert werden. Gleichzeitig ist es notwendig, die Archivierung den rechtlichen Rahmenbedingungen anzupassen. Um dem gerecht zu werden, ist es empfehlenswert, eine Verfahrensdokumentation zu erstellen, welche den Prozess vom Eingang eines Dokuments bis hin zu dessen Archivierung darlegt. Dadurch werden die einzelnen Stationen im Ablage- und Archivierungsprozess deutlich, welche sodann Schritt für Schritt auf ihre Übereinstimmung mit den gesetzlichen Anforderungen überprüft werden können.

Elektronische Rechnungen unterliegen strengen Aufbewahrungs- und Archivierungspflichten, was vielen nicht bewusst ist. Grundsätzlich gelten für elektronische Rechnungen dieselben Aufbewahrungspflichten wie für Papierrechnungen. Das heisst, auch elektronische Rechnungen müssen zehn Jahre lang aufbewahrt werden. Elektronische Rechnungen und Belege müssen zwingend elektronisch archiviert werden. Es genügt nicht, die Unterlagen auszudrucken und in Papierform aufzubewahren. Bei der Umstellung auf die Cloud gilt es daher, genau zu überprüfen, ob der Cloud-Anbieter jene gesetzlichen Aufbewahrungspflichten garantieren kann.

VI. Fazit: erste Arbeitserfahrung

Die Umstellung ist erstaunlich reibungslos verlaufen. Es konnte aber einen Arbeitstag lang nicht gearbeitet werden. Das Überspielen der Daten auf den Server dauerte länger als geplant. Dies verlangsamte die Leitung in den ersten Tagen und führte dazu, dass die Arbeitsplätze nicht so schnell liefen wie gewünscht. Hinzu kam, dass unser Internetprovider noch nicht die volle Leistung erbringen konnte bzw. sich die Erhöhung der Leistung noch etwas verzögert hatte. Den grossen Nachteil der Cloud bekamen wir also bereits in den ersten Tagen zu spüren, nämlich die Abhängigkeit von einer schellen Internetverbindung. Da der Anbieter die gesamte Ordnerstruktur, das Plato samt Daten migrierte und auch bereits die E-Mail-Konten eingerichtet hatte, konnte bis auf ein paar Kleinigkeiten nahtlos weitergearbeitet werden.