www.jusletter.ch

Wolfgang Straub

Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei

Am 30. März 2017 hat der Bernische Anwaltsverband – als erster schweizerischer Anwaltsverband überhaupt – ein Webinar veranstaltet. Dabei ging es um Fragestellungen rund um den Informatikeinsatz in der Anwaltskanzlei. Das Webinar wurde von Simone Kaiser und Fritz Rothenbühler, Präsident des Bernischen Anwaltsverbands, initiiert und moderiert. Im Beitrag werden wichtige Themen aus der Diskussion mit Wolfgang Straub nochmals in schriftlicher Form aufgenommen und mit weiterführenden Literaturhinweisen ergänzt. Der Interviewstil wurde jedoch beibehalten. Zudem finden Sie im Anhang eine Checkliste zu Cloud-Verträgen in der Anwaltskanzlei.

Beitragsarten: Tagungsberichte
Rechtsgebiete: Notariats- und Anwaltsrecht; Informatikrecht

Zitiervorschlag: Wolfgang Straub, Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei, in: Jusletter 1. Mai 2017

ISSN 1424-7410, http://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

► Ist die Digitalisierung eher Fluch oder Chance für die Anwältinnen und Anwälte?

[Rz 1] Die Digitalisierung wird oft als eine plötzlich hereinbrechende, bedrohliche Welle betrachtet, welche kaum eine Branche verschont und nur den Allerfittesten eine Chance zum Überleben lässt. Dieses Bild erscheint in Bezug auf die Anwaltsbranche völlig unzutreffend: Die Bernischen Anwälte werden in absehbarer Zeit kaum durch LegalTech-Expertensysteme ersetzt werden. Vielmehr ist die Frage, wie man die Chancen, welche IT Unterstützung bietet, zur Rationalisierung von Büroabläufen und zur Verbesserung der Dienstleistungen nutzen kann, insbesondere durch eine bessere Verfügbarkeit von dossierbezogenen und juristischen Informationen.[1] In einer Zeit erhöhten Wettbewerbs – der jedoch weniger mit der Digitalisierung als mit der grösseren Anwaltsdichte und dem gesteigerten Kostenbewusstsein der Klienten zusammenhängt – sind sowohl höhere Kosteneffizienz als auch bessere Dienstleistungsqualität durchaus relevant. Optimale Nutzung der IT ist jedoch nur einer von vielen Wettbewerbsfaktoren.

► Welche Strategien machen in Bezug auf die IT Sinn?

[Rz 2] Jede Kanzlei sollte eine IT Strategie erarbeiten, welche zur Ausrichtung der Kanzlei passt.[2] Dabei geht es weniger darum, ein umfangreiches Dokument zu erstellen, als die richtigen Fragen zu stellen. Dazu gehören insbesondere folgende Kernfragen:

- Welche Bedürfnisse haben wir kanzleiintern? Wie können wir die Erwartungen der Klienten am besten erfüllen?
- Wie sehen die bürointernen Abläufe und Prozesse aus (z.B. von der Abklärung von Interessenskollisionen bis zur Archivierung eines Dossiers)?
- Welche Geräte, Programme und Systeme sind heute im Einsatz?
- Welche Kosten und Risiken sind damit verbunden?
- Wie können unsere Bedürfnisse allenfalls besser, günstiger oder risikoärmer erfüllt werden? Welche Ressourcen (personell und finanziell) sind wir bereit, einzusetzen?

[Rz 3] Die Analyse sollte somit Interessen, Prozesse, IT Inventar, Kosten und Risiken sowie Optimierungsmöglichkeiten umfassen.

► Lohnen sich Investitionen in die Informatik überhaupt?

[Rz 4] Die Frage kann nicht so abstrakt beantwortet werden: Je nach Kanzleigrösse bzw. Häufigkeit der einzelnen Abläufe lohnt sich eine Automatisierung.

[Rz 5] Man kann die Frage aber auch umkehren: In welchen Bereichen können wir es uns leisten, auf den Informatikeinsatz zu verzichten? Hier ein paar Beispiele aus unserer Kanzlei:

- Wir haben den Personalaufwand in den letzten 10 Jahren stark reduziert – was nicht nur, aber auch dank Effizienzsteigerungen durch IT – möglich war. Beispielsweise konnten wir den Aufwand bei der Verbuchung von Zahlungen erheblich reduzieren: Früher wurde jede Zahlung zuerst in der Branchensoftware, dann in der Finanzbuchhaltung eingegeben und schliesslich manuell eine Mehrwertsteuerabrechnung erstellt. Heute werden die Zahlungsfiles von Bank und Postfinance direkt in die Branchensoftware importiert, automatisch Klient/Dossier zugeordnet und an die Fibu-Software weitergegeben, aus welcher dann schliess-

1 Siehe dazu auch Gian Sandro Genna, Sind wir Anwälte fit für die Digitalisierung? Anwaltsrevue 2/2017, S. 55–62; Christian Laux, The end of lawyers – Ableitung aus Susskinds Thesen mit Blick auf IT in der Anwaltskanzlei, Anwaltsrevue 1/2015, S. 5–17.

2 Siehe dazu auch Wolfgang Straub, Was bringt IT in der Anwaltskanzlei? Teil 2, Anwaltsrevue 1/2013, S. 21–26, S. 25ff.; Laux Christian, Planung von Kanzlei-IT, Anwaltsrevue 2/2015, S. 69–77.

lich die Mehrwertsteuerabrechnung erstellt wird. Durch den Wegfall der Medienbrüche reduziert sich auch das Fehlerrisiko beim Abtippen von Zahlenreihen. Das Einrichten der Schnittstelle mit der Zuordnung der einzelnen Rechnungspositionen zu den betreffenden Konti der Buchhaltung ist allerdings mit hohem Aufwand verbunden. Zudem gibt es laufend neue Herausforderungen (z.B. in Zusammenhang mit der Einrichtung der elektronischen Rechnungstellung, welche von den Klienten zunehmend verlangt wird).

- Wir arbeiten an zwei Standorten aber mit einer einheitlichen IP-basierten Telefonanlage. Durch die Vernetzung können wir die Telefonanrufe mit weniger Personal je Standort entgegen nehmen.
- Zudem arbeiten wir oft büroübergreifend mit anderen Anwälten zusammen. So sind wir darauf angewiesen, dass die Kommunikation reibungsfrei funktioniert (z.B. Austausch umfangreicher Vertragsdokumente).

[Rz 6] Für grössere Kanzleien sind vor allem die Auswertungsmöglichkeiten der Leistungserfassung interessant, weil sich so rasch feststellen lässt, wie profitabel einzelne Mandate und Mitarbeitende sind.

► Was kann IT Unterstützung für die eigentliche Anwaltsarbeit bieten?

[Rz 7] Leider – oder zum Glück – lässt sich bei der eigentlichen Anwaltsarbeit nur wenig automatisieren. Wir arbeiten zwar mit Standardvorlagen für häufig gebrauchte Dokumente wie Mandatsvertrag, Rechtschriften oder Beilagenverzeichnisse, in welche automatisch die im Dossier hinterlegten Informationen zu Klienten, Gegenparteien etc. eingefügt werden – aber die spezifisch juristischen Inhalte müssen immer wieder einzelfallbezogen erarbeitet werden.

[Rz 8] Bei der juristischen Arbeit geht es vor allem darum, dass die relevanten Informationen im Dossier wie auch in Literatur und Rechtsprechung möglichst effizient gefunden werden.

► Welchen Nutzen bieten elektronische Eingaben bei Gerichten?

[Rz 9] Elektronische Eingaben haben theoretisch einige Vorteile:[3]

- Fristen können bis Mitternacht von jedem beliebigen Standort aus gewahrt werden.
- Zudem lässt sich im Unterschied zu einer Posteinschreibequittung genau beweisen, welche Dokumente wann eingereicht worden sind.

[Rz 10] Diesen stehen aber auch Aufwand und Risiken gegenüber:

- Man muss sich regelmässig auf der Plattform einloggen, um prozessbezogene Dokumente selbst herunterzuladen.
- Zudem trägt man das Risiko eines Ausfalls der Internetverbindung oder technischer Probleme beim Einloggen, Signieren oder Übermitteln.

[Rz 11] Elektronische Eingaben sind bei den Gerichten teilweise immer noch unbeliebt und mit technischen und rechtlichen Besonderheiten verbunden, die es zu beachten gilt (z.B. wurden elektronisch eingereichte Eingaben von einzelnen Gerichten teilweise wiederum kostenpflichtig ausgedruckt und kopiert). Wer Fristen kurz vor Mitternacht durch eine elektronische Eingabe

3 Andrea Schafer, Elektronischer Rechtsverkehr: von der Vision zum Durchbruch, Anwaltsrevue 2012, S. 97 f; Felix Hunziker-Blum, Elektronische Eingaben und SuisseID: Risikovermeidung oder Technologienutzung, Anwaltsrevue 2011, S. 220–222; Stefan Stulz, Elektronische Eingaben und Unterschriften, SuisseID: Lücken, Tücken und erste Erfahrungen, Anwaltsrevue 2011, S. 76–78; Peter Guyan/Lukas Huber, Elektronischer Rechtsverkehr nach VeÜ-ZSSchK, AJP 2011, S. 74–83; Adrian Rufener, Elektronischer Behördenverkehr – Nutzen der SuisseID, Anwaltsrevue 2011, S. 269–271; Jacques Bühler, Effiziente elektronische Kommunikation mit Gerichten, Anwaltsrevue 2009, S. 304–306.

wahren möchte, tut gut daran, die Abläufe vorher ein paarmal ohne Zeitdruck zu üben. Meines Erachtens fehlt es an einem entsprechenden «Playgroundsystem», mit welchem man ausserhalb eines laufenden Verfahrens Erfahrungen sammeln könnte. Dies könnte dazu Beitragen, die Hemmschwellen abzubauen.

► Lohnt es sich, die IT Infrastruktur selbst zu betreiben oder geht man besser gleich in die Cloud?

[Rz 12] IT Outsourcing ist für den Leistungsbezüger eine anspruchsvolle Aufgabe. Wenn man sich als KMU nicht einfach mit einem standardisierten Angebot zufrieden geben will, stehen die Transaktionskosten rasch in einem Missverhältnis zu den erzielbaren Einsparungen. In unserer Kanzlei möchten wir zudem ein gewisses Grundwissen im Umgang mit IT im Haus behalten.

[Rz 13] Man darf sich allerdings nicht täuschen: Fast jede Kanzlei ist auf die Unterstützung von IT Dienstleistern angewiesen, auch diejenigen, welche alles inhouse betreiben. Externe Dienstleister mit Zugang zu Daten müssen durch eine schriftliche Vereinbarung als Hilfspersonen in das Anwalts- und Datengeheimnis eingebunden werden. Es ist aber oft schwierig zu kontrollieren, ob sich die IT Fachleute an Sicherheitsvorschriften und rechtliche Vorgaben halten.

[Rz 14] Durch ein Outsourcing lassen sich Investitionskosten reduzieren und laufende Kosten fallen weitgehend nutzungsabhängig und periodengerecht an. Zudem können auch kleine Kanzleien von einem professionellen IT Betrieb profitieren (z.B. rasches Einspielen von Sicherheitspatches auf den Servern, Management von Firewalls). Bei einem Vergleich der Outsourcinggebühren mit dem Betrieb einer eigenen Infrastruktur dürfen individuelle Anpassungskosten allerdings nicht unterschätzt werden (z.B. Parametrisierungen der Programme, Pflege von Dokumentenvorlagen, Einrichten und Aufrechterhalten von Schnittstellen bei Releasewechseln). Für Kanzleien mit einem hohen IT Integrationsgrad machen diese in der Regel einen erheblichen Teil der Gesamtkosten aus. Hier entsteht zudem eine hohe Abhängigkeit vom Provider, da in der Regel nur dieser in der Lage ist, gewisse Arbeiten vorzunehmen.

[Rz 15] Für Kanzleien, welche heute bereits eine sehr umfassende und moderne IT Infrastruktur betreiben, ist eine Migration zu Cloud Services sehr aufwändig. Hingegen können Cloud Angebote attraktiv sein, wenn die IT der Kanzlei völlig neu aufgebaut werden soll. Dabei sind allerdings rechtliche Rahmenbedingungen zu beachten.[4] Zudem ist der Reduktion der Abhängigkeiten vom Provider besondere Aufmerksamkeit zu schenken (siehe dazu auch die Checkliste an Ende des Beitrages).

---

4 Siehe dazu Wolfgang Straub, Checkliste zu Cloud Verträgen in der Anwaltskanzlei, im Anhang dieses Beitrags, Conseil des barreaux européens (CCBE), Guidelines on the use of cloud computing services by lawyers, www.ccbe.eu; CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud, 4 April 2014; Sébastien Fanti, Cloud Computing: opportunités et risques pour les avocats, Revue de l'avocat 2013 S. 74–77; Adrian Rufener, Cloud Computing, Anwaltsrevue 4/2012, S. 198f.; Adrian Rufener, Arbeiten in der Cloud, Anwaltsrevue 6–7/2013 S. 295f.; Thomas J. Shaw, Cloud Computing for Lawyers and Executives: A Global Approach, 2nd edition, Chicago: American Bar Association, 2013.; Ursula Sury/Yves Goginat, Umzug einer Anwaltskanzlei in die Cloud, Anwaltsrevue 5/2015, S. 201–206 sowie generell zu Cloud Verträgen Wolfgang Straub, Cloud Verträge – Regelungsbedarf und Vorgehensweise, AJP 2014, S. 905–923 und Wolfgang Straub, Cloud Computing – Checkliste zum vertraglichen Regelungsbedarf, in: Jusletter 14. Juli 2014.

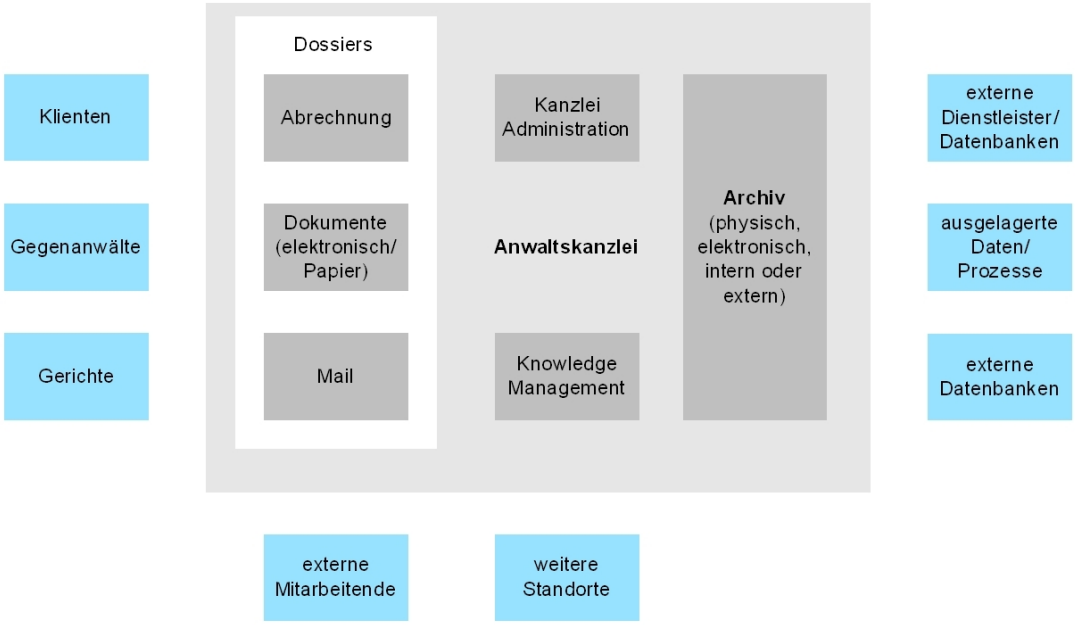

Abbildung 1: Übersicht zum Informationsmanagement in der Anwaltskanzlei

► Und wie steht es mit der Sicherheit?

[Rz 16] IT Sicherheit ist ein komplexes Thema und erfordert in der Regel den Beizug von Spezialisten.[5] Trotzdem dürfen Anwälte nicht alles den IT Fachleuten überlassen. Im Hinblick auf unsere beruflichen Sorgfaltspflichten müssen wir mindestens die branchenüblichen Sicherheitsmassnahmen treffen.

[Rz 17] Es ist grundsätzlich zwischen Vertraulichkeits- und Integritätsaspekten (z.B. Schutz vor Hacking) sowie Verfügbarkeitsaspekten (z.B. Internetausfall) zu unterscheiden.

- Elektronische Dossiers bieten in Bezug auf die *Integrität* spezifische Risiken und Chancen. Alles was digital vorhanden ist, könnte bei einem Hackerangriff auch heruntergeladen werden. Auf der anderen Seite lassen sich irrtümlich oder durch äussere Einwirkungen (z.B. Brand) gelöschte Dokumente anhand von Sicherungskopien mit wenig Aufwand wiederherstellen, wenn regelmässig entsprechende Backups gemacht bzw. extern aufbewahrt wurden. Anders als in einem Papierdossier lässt sich via Logfiles auch leichter nachvollziehen, wann welche Dokumente bearbeitet oder gelöscht wurden oder wann Leistungen verbucht wurden. Die digitale Nachvollziehbarkeit kann allenfalls auch präventiven Nutzen haben, wenn Mitarbeitende die Kanzlei verlassen.
- In Bezug auf die *Verfügbarkeit* von Internetanschlüssen gibt es grundsätzlich zwei Vorgehensstrategien: Technische Absicherung durch Redundanz und vertragliche Absicherung durch Serviceverträge mit garantierten Wiederherstellungszeiten. Hier gilt es den richtigen Mix zu finden.

5 Siehe dazu David Rosenthal, IT-Sicherheit in der Anwaltskanzlei, Anwaltsrevue 2006, S. 281–288 und 323-330.

► Sollte die Kommunikation mit Klienten und Gegenanwälten stets verschlüsselt werden?

[Rz 18] Das ist ein leidiges Thema.[6] Die Art der Kommunikation sollte explizit im Mandatsvertrag geregelt werden.[7]

[Rz 19] Es ist grundsätzlich zwischen der Verschlüsselung des Transportwegs, der Verschlüsselung von E-Mails und der Versendung von verschlüsselten Dokumenten zu unterscheiden. Auf Wunsch einzelner Klienten haben wir in unserer Kanzlei zahlreiche Verschlüsselungsmethoden für E-Mails ausprobiert, aber bisher keine Lösung gefunden, welche wir flächendeckend einsetzen. Meist wünschen die Klienten nach kurzer Zeit wieder eine Umstellung auf unverschlüsselten Mailverkehr, weil der verschlüsselte mit Komforteinschränkungen verbunden war. In einigen Mandaten nutzen wir SharePoint Server auf Klientenseite, d.h. alle mandatsbezogenen Dokumente müssen dort heruntergeladen bzw. wieder hochgeladen werden.

► Wie sollten E-Mails archiviert werden?

[Rz 20] Ein grosser Teil der Geschäftskorrespondenz wird heute nur noch elektronisch abgewickelt. Nicht allen Anwälten ist bewusst, dass sie – jedenfalls soweit eine Eintragungspflicht im Handelsregister besteht – auch die Vorschriften der Geschäftsbücherverordnung eingehalten werden müssen. Diese enthält detaillierte Anforderungen an die Archivierung elektronischer Dokumente. Einige Anwälte dürften den Buchführungsvorschriften auch deshalb unterstehen, weil sie mit ihrer Büroinfrastruktur Geschäftskorrespondenz für selbst verwaltete Gesellschaften abwickeln. Zudem bestehen berufsrechtliche Vorschriften zur Aktenaufbewahrung, welche allenfalls zu einer analogen Anwendung von Bestimmungen der Geschäftsbücherverordnung führen könnten.[8]

---

6 Siehe zur Frage der E-Mail-Verschlüsselung in Anwaltskanzleien Wolfgang Straub, Was bringt IT in der Anwaltskanzlei? Teil 1, Anwaltsrevue 11–12/2012, S. 521–525, S. 522ff.; Adrian Rufener, Automatisation/IT: Neue Möglichkeiten in der Prozessunterstützung von Anwaltskanzleien, in: Leo Staub/Christine Hehli Hidber (Hrsg.): Management von Anwaltskanzleien: erfolgreiches Führen von Anwaltsunternehmen, Zürich 2012, S. 337–353, Rz. 13 f.; Adrian Rufener, Mailsicherheit, Anwaltsrevue 2011, S. 380; Sébastien Fanti, Courrier électronique et responsabilité de l'avocat, Anwaltsrevue 2011, S. 492–493; Kaspar Schiller, Schweizerisches Anwaltsrecht, Grundlagen und Kernbereich, Bern 2009, Rz. 539; Adrian Rufener, Sicherer Mailverkehr: eine Frage der Professionalität, Anwaltsrevue 2009, S. 191–194; David Rosenthal (Fn. 5), S. 326f.; Sarah Montani / Franz Kummer, Vor E-Mail sind wir alle gleich, in: Jusletter 21. Juni 2004; Robert G. Briner, Anwaltliche Sorgfaltspflichten und E-Mail, SJZ 2005, S. 437–435; Wolfgang Wiegand, Die Sorgfalts- und Informationspflichten bei der Erbringung von Rechtsdienstleistungen unter Verwendung von Internet und E-Mail, in: Thomas Koller/Hanna Muralt Müller (Hrsg.), Tagung 2000 für Informatik [und] Recht, Bern 2001, S. 149–172; Fridolin Walther, Das Anwaltsgeheimnis im E-Mail-Zeitalter – eine Problemskizze, SJZ 2000, S. 357–366, und SJZ 2001, S. 65–66; Oliver Blum, Das Anwaltsgeheimnis im E-Mail Zeitalter, Eine Entgegnung aus der Praxis, SJZ 2000, S. 550–552, und SJZ 2001, S. 67 f.

7 Siehe dazu im Einzelnen Wolfgang Straub, Mandatsvereinbarungen und IT – was ist zu regeln? Anwaltsrevue 3/2013, S. 124–128.

8 Siehe den Fragestellungen rund um die Archivierung Ivan Oppliger / Christophe von Werdt, Digitale Aktenablage und digitales Archiv in der Anwaltskanzlei, Anwaltsrevue 2/2015, S. 69–77; Wolfgang Straub, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP 2010, S. 547–564; Lukas Fässler, Mandatsinformationen digital verwalten und archivieren, Anwaltsrevue 5/2013, S. 233–238.

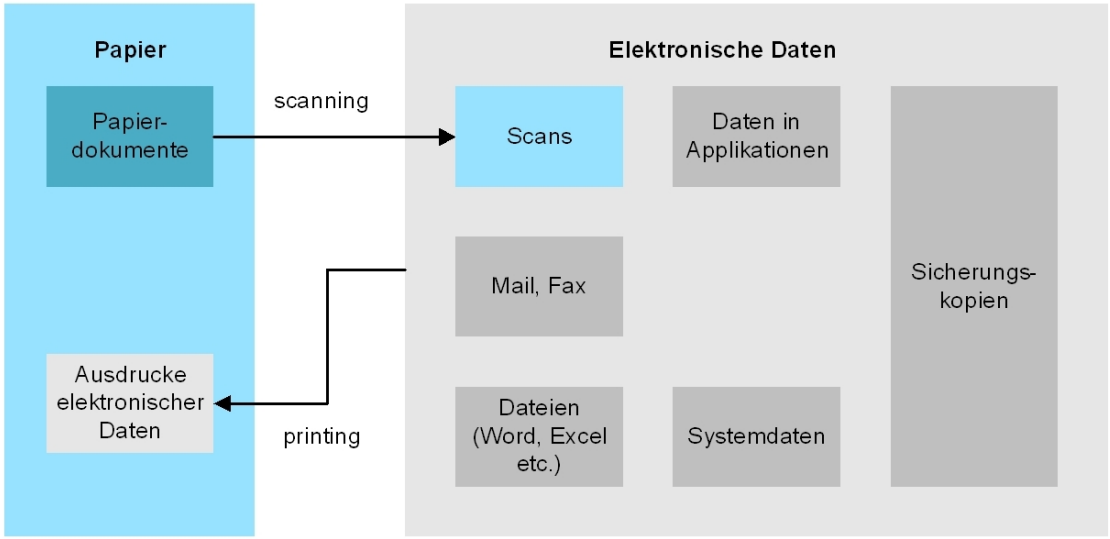

Abbildung 2: Analoge und elektronische Daten in der Anwaltskanzlei

► Genügt es nicht, einfach alle E-Mails auszudrucken?

[Rz 21] Eine Aufbewahrung in der Form von Papierausdrucken ist zunehmend schwieriger zu gewährleisten (z.B. von mobilen Geräten aus versandte E-Mails) und oft auch gar nicht sinnvoll. Solche Dokumente müssen nämlich in nicht veränderbarer Form gespeichert werden. Zudem muss sich nachweisen lassen, wann ein E-Mail ein- oder ausgegangen ist. Die entsprechenden Informationen müssen während der ganzen 10-jährigen Aufbewahrungsdauer lesbar bleiben.[9] Diese Anforderungen können nur mit speziellen Mailarchivierungsprogrammen erfüllt werden. Wir haben uns bereits 2007 zur Einführung einer solchen Lösung entschieden. Diese hat sich im Alltag als sehr praktisch erwiesen, da sie die Rückverfolgung von Maildialogen erlaubt und auch alle Attachments mit aufzeichnet. So kann auf einfache Weise nach Stichworten, Zustellungsinformationen und nicht mehr auf dem Mailserver vorhandenen E-Mails gesucht werden.

► Wie können Telefaxe in die Archivierung einbezogen werden?

[Rz 22] Alle ein- und ausgehenden Faxe werden auf ein eigenes Mailkonto kopiert. Damit werden Fax und E-Mail zugleich so kanalisiert, dass diese Dokumente auch beim Arbeiten von ausserhalb des Büros via Terminalserver verfügbar sind. Der Hauptvorteil dieser Lösung liegt aus meiner Sicht darin, dass Faxe ohne grossen Aufwand in die E-Mailarchivierung einbezogen werden. Allerdings hat die praktische Bedeutung des Telefax in den letzten Jahren stark abgenommen.

9 Siehe dazu Wolfgang Straub, Mandatsvereinbarungen und IT (Fn. 7), S. 124 ff. sowie die Mustervorlagen auf www.it-recht.ch.

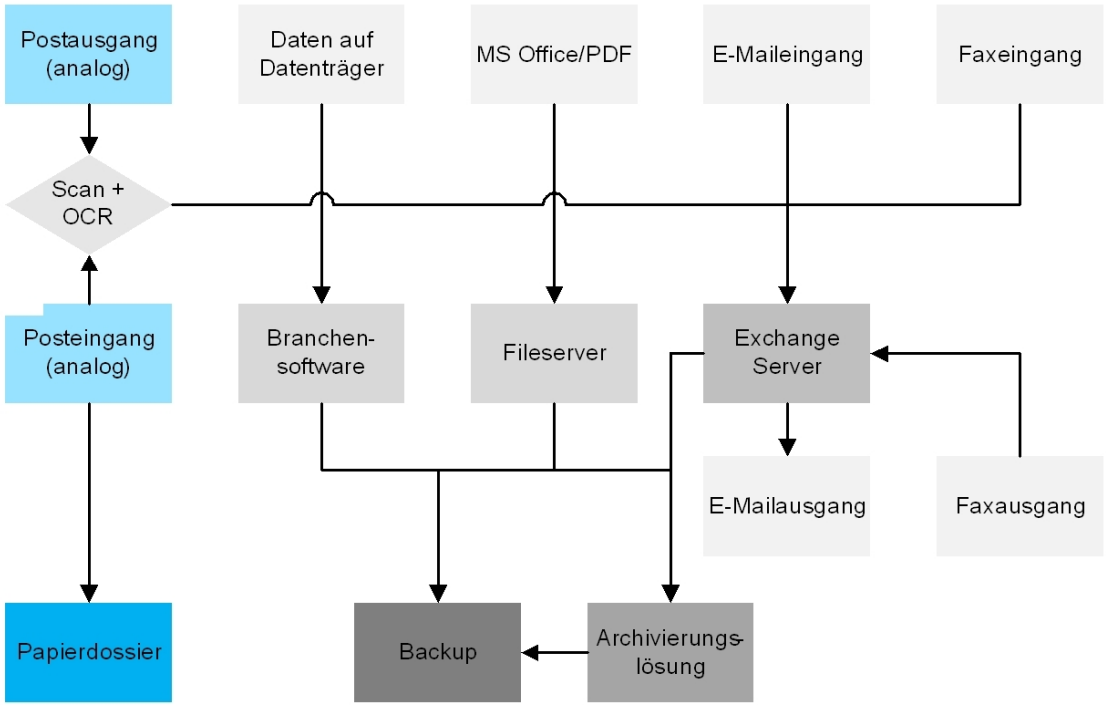

Abbildung 3: Beispiel zur elektronischen Archivierung

► Haben eingescannte Dokumente den gleichen Beweiswert wie Papierdokumente?

[Rz 23] Dies ist eine sehr komplexe Frage, welche je nach Rechtsgebiet und Inhalt des betreffenden Dokuments beantwortet werden muss.[10] Ebenso wie Papierurkunden sind auch Scans in Zivil-, Straf- und Verwaltungsprozessen stets Gegenstand einer richterlichen Beweiswürdigung. Scanning bedeutet einen Medienbruch. Durch das Einscannen gehen immer gewisse Informationen verloren (z.B. chemische Zusammensetzung der Tinte in Unterschriften). Auf diese kommt es aber nur in den seltensten Fällen an (z.B. Strafprozesse über Urkundenfälschung). Hingegen stellen sich in Bezug auf Scans von Originaldokumenten zusätzliche Fragen:

- Wurde das Originaldokument vor dem Einscannen geändert? Dokumente sollten daher möglichst rasch nach der Erstellung/dem Eingang gescannt werden.
- Ist der Scan vollständig (z.B. Vor- und Rückseiten, Farbscan, wenn Farben eine Rolle spielen)? Hier ist darauf zu achten, dass der Scanner keine automatischen Bildbearbeitungsfunktionen verwendet, da Geräte mitunter nicht zwischen einem Staubkorn und einem Komma in einer Zahlenreihe unterscheiden können.
- Wann wurde das Dokument gescannt? Dies kann z.B. durch einen Zeitstempel in der Scandatei oder durch Logfiles belegt werden.
- Wurde der Scan nachträglich manipuliert? Es empfiehlt sich, ein unveränderbares Format zu verwenden (z.B. PDF/A). Allfällige Nachbearbeitungsschritte an Scans sollten dokumentiert werden (z.B. Einbettung der Originaldatei in die bearbeitete Datei).
- Wichtige Urkunden sollten nach dem Scannen nicht vernichtet, sondern gegebenenfalls den Klienten zurückgegeben werden.

10 Siehe dazu Lukas Fässler, Elektronische Aktenführung – Beweisführung mit eingescannten Dokumenten, Anwaltsrevue 9/2014, S. 380–385.

- Der Scanprozess sollte innerhalb der Kanzlei standardisiert und dokumentiert werden. Dabei kann allerdings unterschiedlich hoher Aufwand betrieben werden. In Deutschland gibt es bereits eine Norm zum rechtssicheren Scannen. Eine Umsetzung der Technischen Richtlinie 03138 des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) über «rechtssicheres ersetzendes Scannen» ist allerdings aufwändig und eher für die einmalige Digitalisierung grosser Aktenbestände als für das tägliche Scannen von Anwaltskorrespondenz geeignet.

► Lässt sich der ganze Prozess nicht einfach z.B. an die Post auslagern?

[Rz 24] Eine Auslagerung des Scannens der eingehenden Post an externe Dienstleister ist grundsätzlich möglich, doch müssen diese als Hilfspersonen ins Anwaltsgeheimnis eingebunden werden. Zudem ist sicherzustellen, dass wichtige Urkunden (z.B. eingehende Originalurteile) nach dem Scannen nicht vernichtet sondern der Kanzlei weitergeleitet werden.

► Was sind die Herausforderungen bei der elektronischen Archivierung?

[Rz 25] Eine der grössten Herausforderungen ist wohl, dass klientenbezogene analoge und elektronische Informationen gleichzeitig an verschiedenen Orten entstehen (z.B. E-Mails, Papierkorrespondenz, Ablagen einzelner Mitarbeitender auf lokalen Geräten und Ordnern auf Servern). Voraussetzung für eine zuverlässige elektronische Archivierung von klientenbezogenen Informationen ist daher eine Kanalisierung in einem zentralen elektronischen Dossier.

[Rz 26] Neben den Klientendossiers müssen aber auch zahlreiche kanzleibezogene analoge und elektronische Informationen archiviert werden (z.B. AHV-Abrechnungen, Mehrwertsteuerabrechnungen, Steuererklärungen etc.). Um ein sinnvolles Archivierungskonzept zu erarbeiten, sollten daher zuerst die Prozesse und die Ablagen analysiert werden.

► Wann beginnen die Aufbewahrungspflichten?

[Rz 27] Je nach Rechtsnorm sind hier unterschiedliche Anknüpfungen zu beachten:

- Die berufsrechtlichen Aufbewahrungspflichten beginnen mit Abschluss des Dossiers, was bei Anschlussfragen und konnexen Mandaten schwierige Fragen aufwerfen kann (und gegebenenfalls für die Eröffnung eines neuen Mandats spricht).
- Demgegenüber stellen die steuerrechtlichen Vorschriften auf das Geschäftsjahr ab, auf welches sich die Dokumente beziehen.

► Sind die berufsrechtlichen Aufbewahrungspflichten zwingender Natur?

[Rz 28] Da sie dem Schutz der Klienteninteressen dienen, sind sie m.E. dispositiv und können vertraglich sowohl verkürzt als auch verlängert werden. Eine solche Vereinbarung hat aber keinen Einfluss auf allfällige parallele kaufmännische, steuer- oder sozialversicherungsrechtliche Aufbewahrungsdauern.

► Müssen auch blosse Mandatsanfragen und Unterlagen zu Gratisauskünften archiviert werden?

[Rz 29] In Bezug auf solche Unterlagen ist m.E. zu differenzieren:

- Der Mandatsvergabe gehen unter Umständen längere Verhandlungen voraus, in deren Rahmen mitunter bereits sensitive Informationen offen gelegt werden. Die potenziellen Klienten müssen darauf vertrauen können, dass diese nicht gegen sie verwendet werden, auch wenn das Mandat – aus welchen Gründen auch immer – schliesslich nicht zustanden kommt. Solche Informationen können allenfalls zu Interessenskollisionen führen und sind insoweit be-

rufsrechtlich aufbewahrungspflichtig als die Interessenten nicht eine Rückgabe/Vernichtung verlangt haben.
- Für die berufsrechtlichen Aufbewahrungspflichten spielt es keine Rolle, ob viel oder wenig oder gar kein Honorar vereinbart oder bezahlt wurde.
- Steuerrechtliche Aufbewahrungspflichten knüpfen demgegenüber an einem steuerbaren Entgelt an.
- Im Hinblick auf Auftragsrecht und kaufmännische Buchführungspflichten ist zudem zu beachten, dass auch Gratisleistungen Haftungsansprüche auslösen können.

► Gibt es in bestimmten Konstellationen sogar eine Pflicht zur Erstellung elektronischer Backups?

[Rz 30] Diesbezüglich ist zu unterscheiden, in welcher Form die Informationen vorliegen:

- Grundsätzlich gibt es m.E. keine Pflicht, Papierakten einzuscannen. Aus der Sorgfaltspflicht folgt allerdings auch, dass anvertraute Unterlagen gegen zufällige Vernichtung (z.B. durch Elementarschäden) und Diebstahl geschützt werden.[11] Bei sehr wichtigen Dokumenten könnte sich daraus unter Umständen auch eine Pflicht ergeben, Kopien (in analoger oder digitaler Form) zu erstellen und an einem anderen Standort aufzubewahren (z.B. Banksafe).
- Liegen Daten aber einmal in elektronischer Form vor, so sind sie entsprechend den heute üblichen Sorgfaltsmassstäben zu sichern. Dazu gehören das regelmässige Erstellen von Backups und die periodische externe Lagerung solcher Kopien (z.B. Festplatte oder Tape in einem Banktresor oder Erstellung einer Sicherungskopie in einem externen Rechencenter).

► Wie müssen verschlüsselte Informationen aufbewahrt werden?

[Rz 31] Hier stellen sich in der Praxis schwierige Fragen. Vorab ist zwischen der Verschlüsselung von Dokumenten, Mails etc. und der blossen Verschlüsselung des Transportwegs zu unterscheiden. Wenn ein Dokument nur in verschlüsselter Form vorliegt (z.B. verschlüsseltes Mailattachment), so muss der entsprechende Schlüssel gleich wie das Dokument selbst aufbewahrt werden. Zudem ist sicherzustellen, dass das Dokument während der gesetzlichen Aufbewahrungsdauer jederzeit entschlüsselt werden könnte. Das kann dann zu praktischen Problemen führen, wenn die entsprechende Software inzwischen ersetzt wurde. Wenn eine Datenmigration auf ein neues System erfolgt oder unverschlüsselte Kopien der Dokumente erstellt werden, so ist es wichtig, den entsprechenden Prozess klar nachvollziehbar zu dokumentieren.

► Müssen die Mailaccounts aller Kanzleimitarbeitenden in die Archivierung einbezogen werden? Besteht hier nicht die Gefahr von Persönlichkeitsverletzungen?

[Rz 32] Es kann zwar eine Weisung erlassen – und den Mitarbeitenden periodisch wieder in Erinnerung gerufen – werden, wonach private und geschäftliche Mails zu trennen sind. In der Praxis dürfte es aber immer wieder zu Vermischungen kommen. Daher sollten geschäftsrelevante Mails am besten in ein Dokumentenmanagementsystem verschoben und dort dem jeweiligen Dossier zugeordnet werden – auf diese Weise werden sie auch für andere Kanzleimitarbeitenden sichtbar.

► Müssen sogar Spam-Ordner archiviert werden?

[Rz 33] Was als lesenswertes Mail in den Posteingang kommt und was in den Spamordner verschoben oder gelöscht wird, bestimmen die entsprechenden Algorithmen im Mailserver bzw. der Firewall. Dies führt immer wieder zu Fehlzuordnungen, so dass auch für die Mandatsführung

11 Siehe dazu auch Urteil des Bundesgerichts 5P.162/2003 vom 21. Mai 2003.

relevante Mails mitunter fälschlicherweise als Spam behandelt werden. Um den gesamten Mailverkehr sicher rekonstruieren zu können, sollten daher auch Spamordner ab und zu angeschaut und in die Archivierung einbezogen werden. Zudem können, die Systeme so konfiguriert werden, dass den Versendern eine automatische Nichtzustellungsmitteilung gesendet wird. So kann eine allfällige Pflicht zu reagieren gegebenenfalls auf den Mailabsender verlagert werden.

► Und wie sieht es aus, wenn Anwälte die Kanzlei verlassen, in andere Kanzleien wechseln, oder wenn sich Kanzleien aufspalten oder fusionieren?

[Rz 34] Hier stellen sich viele komplexe Fragen, welche nicht in wenigen Sätzen beantwortet werden können. M.E. ist berufsrechtlich zwischen mandatsverantwortlichen Anwälten und sonstigem Personal zu unterscheiden. In Bezug auf Buchführungs- und Steuerrecht ist hingegen relevant, ob der betreffende Anwalt bzw. die betreffende Anwältin oder die Kanzlei Steuersubjekt war. Berufsrechtlich müssen ausscheidende Anwälte grundsätzlich weiterhin feststellen können, ob sie neue Mandate wegen Interessenskollisionen aufgrund bisher von ihnen geführten Mandaten ablehnen müssen.

► Können Informationen auch zu lange aufbewahrt werden?

[Rz 35] Datenschutzrechtlich besteht ein Vernichtungsanspruch am Ende der gesetzlichen Aufbewahrungsdauern. Hier ist aber m.E. eine Interessensabwägung zwischen dem Vernichtungsinteresse und den anderen beteiligten Interessen vorzunehmen (insbesondere der Verpflichtung, Interessenskollisionen in künftigen Mandaten abklären zu können). Unter Umständen haben aber auch Klienten ein Interesse an einer längeren Aufbewahrung – etwa im Hinblick auf spätere Anschlussfragen. Die Frage sollte daher in der Mandatsvereinbarung geregelt werden.

[Rz 36] Schwierige Fragen stellen sich auch in Bezug auf die Löschung bestimmter Daten in Backupmedien. Solche Massnahmen können äusserst aufwändig und unter Umständen rechtlich problematisch sein kann (Integritätsschutz der Datenträgerinhalte). M.E. genügt hier in der Regel ein Wiederherstellungsverbot der betreffenden Daten auf die Produktivsysteme. Dieses ist z.B. durch entsprechende Weisungen und Vermerke zu dokumentieren.

► Wie lassen sich elektronische Akten sicher wieder vernichten?

[Rz 37] Sowohl für die Vernichtung von Papierakten (insbesondere Schnipselgrösse) als auch von Datenträgern gibt es Normen (z.B. DIN 66399:2012 «Vernichtung von Datenträgern»).[12] Ob diese bei Anwaltskanzleien bekannt sind und berücksichtigt werden, ist jedoch fraglich. Aus meiner Sicht kommt es weniger darauf an, ob eine bestimmte Norm eingehalten wird, sondern dass es in der Kanzlei standardisierte Prozesse gibt, wie mit zu vernichtenden Daten oder Datenträgern umgegangen wird. Diese können z.B. in einem IT oder Informationssicherheitskonzept festgehalten werden.

[Rz 38] Bei einer Löschung werden oft nur die Indexdateien, nicht aber die Daten selbst überschrieben. Wiederbeschreibbare Datenträger sollten daher unter Verwendung von zufälligen Datenmustern mehrmals überschrieben werden.

[Rz 39] Anwälte sind sich manchmal zu wenig bewusst, dass auch in Kopiergeräten, Handys etc. Datenträger eingebaut sind, welche am Ende der Lebensdauer sicher vernichtet werden müssen.

---

12 Siehe dazu im Einzelnen Maria Winkler, Daten- und Aktenvernichtung in der Anwaltskanzlei, Anwaltsrevue 6–7/2015, S. 275–279.

[Rz 40] Wenn elektronische Daten bei einem externen Dienstleister gespeichert werden, muss auch der Prozess der Datenvernichtung (inkl. Backupmedien) verbindlich geregelt und dokumentiert werden. Zudem müsste gemäss EDÖB ein Kontrollrecht vereinbart werden. Für kleine Kanzleien dürfte es jedoch schwierig sein, diese Anforderung gegenüber einem grossen Provider durchzusetzen.

Anhang

Die Checkliste zum Webinar «Keller oder Wolke? – Digitales Arbeiten in der Anwaltskanzlei» finden Sie direkt an diesen Beitrag angehängt.

Den Podcast zum Webinar «Keller oder Wolke? – Digitales Arbeiten in der Anwaltskanzlei» finden Sie **hier**.

Autor und Referierende:
Wolfang Straub, Dr. iur., LL.M., Fürsprecher, ist Rechtsanwalt in Bern und Lehrbeauftragter am CAS ICT Beschaffungen der Universität Bern.

Simone Kaiser, IR, RA, EMBA, ist Verlagsleiterin der Editions Weblaw.

Fritz Rothenbühler, Dr. iur., Fürsprecher, ist Rechtsanwalt in Bern und Präsident des Bernischen Anwaltsverbands.

www.jusletter.ch

Wolfgang Straub

Checkliste zu Cloud Verträgen in der Anwaltskanzlei

Die vorliegende Checkliste ergänzt den Beitrag, «Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei» im Jusletter vom 1. Mai 2017

Beitragsarten: Tagungsberichte
Rechtsgebiete: Notariats- und Anwaltsrecht, Informatikrecht

Zitiervorschlag: Wolfgang Straub, Checkliste zu Cloud Verträgen in der Anwaltskanzlei, in: Jusletter 1. Mai 2017

[Rz 1] Der Einsatz von Cloud Services in der Anwaltskanzlei wirft eine Vielzahl von Rechtsfragen auf. Einige – aber nicht alle – dieser Fragen lassen sich vertraglich regeln. Die vorliegende Checkliste[1] versteht sich als Ergänzung zu einer systematischen Vorgehensmethodik, welche folgende Elemente umfasst:[2]

- Analyse der Interessenlage
- Bestimmung des auszulagernden Bereiches
- Analyse der rechtlichen Anforderungen und der notwenigen Ressourcen
- Analyse der wirtschaftlichen, technischen und rechtlichen Chancen und Risiken
- Festlegung der Kriterien für die Auswahl und die Zusammenarbeit mit dem Provider
- Regelung der Zuständigkeiten und Verantwortlichkeiten zwischen den Parteien
- Instruktion und Überwachung des Providers
- Eventuell Information/Zustimmung der Klienten einholen

[Rz 2] Die vorliegende Checkliste ist auf komplexe Services zugeschnitten. Sie erhebt aber keinen Anspruch auf Vollständigkeit. Wenn die Vertragsbedingungen vom Provider vorgegeben werden, kann die Checkliste helfen, Risiken zu erkennen und darüber zu entscheiden, ob die Konditionen für die beabsichtigte Verwendung akzeptabel sind oder nicht.

1 Siehe auch die Checkliste ‚Cloud Computing' des Zürcher Anwaltsverbandes, sowie die Checkliste des CCBE, Guidelines on the use of cloud computing services by lawyers, www.ccbe.eu

2 Siehe auch STRAUB WOLFGANG, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 7/2014, S. 905 ff. Weitere – nicht anwaltsspezifische – Checklisten zum Cloud Computing finden sich auch in den EUROCLOUD LEITFÄDEN zum Cloud Computing, online verfügbar unter www.eurocloudswiss.ch/index.php/publikationen/leitfaden. Siehe insbesondere den detaillierten Fragekatalog zur Informationssicherheit im Leitfaden Risk & Compliance, Kap. 6, S. 28 ff. Eine Checkliste für Audits findet sich bei HALPERT BEN (Hrsg.), Auditing Cloud Computing: A Security and Privacy Guide, Hoboken NJ 2011, S. 175 ff.

1. Rahmenbedingungen

1.1. Vertragsparteien

1.1.1. *Informationen zum Provider* und seinen Subunternehmern, insbesondere wo die Services erbracht werden und welche nationalen Rechtsvorschriften anwendbar sein können

1.1.2. Informationen zu bestehenden *Zertifizierungen des Providers* und seiner Subunternehmer; Verpflichtung zur Aufrechterhaltung während der Vertragsdauer

1.1.3. *Informationen zur Anwaltskanzlei*, insbesondere an welchen Standorten, von welchen Nutzern (z.B. Mitarbeitende, Klienten) und wofür die Services bezogen werden und welche Rechtsvorschriften anwendbar sein könnten

1.2. Vertragsdokumente und Änderungen

1.2.1. Verzeichnis der *Vertragsbestandteile* und Hierarchie der einzelnen Vertragsdokumente (keine Verweise auf URLs, welche vom Provider einseitig aktualisiert werden können!)

1.2.2. *Form* von Vertragsänderungen (keine einseitigen Änderungsrechte!) und von Erklärungen an die Gegenpartei, welche die Rechtslage gestalten; elektronische Zustellung von Dokumenten (z.B. Rechnungen, Reports, Mitteilungen)

1.3. Begriffsdefinitionen und Verweise auf Standards

1.4. Nebenpflichten und Obliegenheiten

1.4.1. *Mitwirkungs- und Informationspflichten* (z.B. Benachrichtigung bei Leistungseinschränkungen, welche für die Anwaltskanzlei nicht ohne weiteres erkennbar sind); Form des Abrufs und der Abmahnung von Mitwirkungspflichten

1.4.2. Unterstützung von Drittleistungserbringern der Anwaltskanzlei durch den Provider

1.4.3. *Dokumentation* von System und Prozessen

2. Inhalt der Leistung

2.1. Grundlagen

2.1.1. *Beschreibung aller Kanzleistandorte* etc., von denen aus *Zugriffe* auf Daten der Anwaltskanzlei möglich sind

2.1.2. *Beschreibung aller Rechenzentren* etc., in welchen vertragliche Leistungen erbracht werden können (Lokalisierung, Zertifizierung etc.)

2.1.3. Beschreibung der dedizierten Infrastruktur (Private Cloud)

2.1.4. Spezifizierung der zur Verfügung gestellten *Softwareversionen* (Funktionen, Optionen, Customizing-Möglichkeiten etc.)

2.1.5. Deklaration von *Drittleistungen*, welche der Provider anbietet (z.B. Zurverfügungstellen von Software Dritter oder Leistungen externer Infrastructure Service Provider); Offenlegung der Lizenzbedingungen für entsprechende Software und der Service Level Agreements für Wartungs- und Supportleistungen Dritter → Einbezug in Geheimhaltungspflichten

2.1.6. Regelung der *Nutzungsrechte* an vom Provider verwendeter Software bzw. von ihm erbrachten Services. Sofern Drittsoftware im Rahmen von Cloud Services genutzt werden soll, sind dafür entsprechende Lizenzen erforderlich. Können auch allfällige bereits vorhandene Lizenzen der Anwaltskanzlei im Rahmen der Cloud Services verwendet werden? Dies setzt eventuell Erweiterungen/Umwandlungen der Lizenzen voraus.

2.1.7. Regelung der Immaterialgüterrechte an individuellen *Zusatzentwicklungen* für die Anwaltskanzlei

2.1.8. Technische Voraussetzungen auf Seiten der Anwaltskanzlei, Möglichkeiten des Datenimports und -exports, Beschreibung der *Schnittstellen* zu Systemen und Anwendungen der Anwaltskanzlei

2.1.9. *Portierbarkeit* von Applikationen und Daten auf andere Plattformen, Compliance mit Standards

2.1.10. Schulungskonzepte, Anwender- und *Betriebshandbücher*

2.2. Verantwortungsbereiche

2.2.1. Definition der *Verantwortungsbereiche der* Anwaltskanzlei (inhaltliche Verantwortung, Datenherrschaft)

2.2.2. Definition der *Verantwortungsbereiche des Providers* (Leistungserbringung, Umsetzung von Weisungen der Anwaltskanzlei als Erfüllungsgehilfe, technische Schutzmassnahmen etc.)

2.2.3. Subsidiäre Abgrenzungsregeln

2.3. Weisungsrecht

2.3.1. Ist das *Weisungsrecht* der Anwaltskanzlei klar definiert?

2.3.2. Wie ist vorzugehen, wenn *Weisungen der Anwaltskanzlei* nach Auffassung des Providers *gegen* das Datenschutzrecht oder sonstige gesetzliche *Vorschriften verstossen*?

2.3.3. Innerhalb welcher Fristen und in welcher Form müssen *Verstösse des Providers* oder seiner Mitarbeitenden und Subunternehmer gegen gesetzliche Vorschriften, vertragliche Bestimmungen oder Weisungen der Anwaltskanzlei diesem mitgeteilt werden? (siehe auch Ziff. 4.1.2)

2.4. Migration

2.4.1. Beschreibung Initialprojekts sowie einer allfälligen *Migration* (z.B. Ablauf, Projektorganisation, Konflikteskalationsprozedere)

2.4.2. Beschreibung der *Abnahmeprozesse* und der Bedeutung der Abnahmen (Inkraftsetzen von Service Level Agreements, Zahlungsvoraussetzungen, Vertragsausstiegsmöglichkeiten beim Scheitern von Abnahmen etc.)

2.5. Servicebeschreibung

2.5.1. *Beschreibung der Leistungen und Definition der Service Levels,* z.B. Definition von Mindestverfügbarkeiten, Übertragungsbandbreiten, Systemantwortzeiten, Support Levels, Recovery Time Objectives (wie lange darf ein Geschäftsprozess oder ein System ausfallen?), Recovery Point Objectives (wie viel Datenverlust kann in Kauf genommen werden?) und Zufriedenheit der Nutzer durch Key Performance Indicators

2.5.2. Definition von *Wartungsfenstern* (maximale Unterbruchsdauer, Form, Inhalt und Fristen der Vorankündigung)

2.5.3. *Support, Störungs- und Fehlermanagement* (Beschreibung des Behebungs- und Supportprozesses, insbesondere Verfügbarkeit der Hotline, Ticketing, Supportsprachen, Interventions- und Behebungszeiten, Konflikteskalationsprozesse)

2.5.4. *Service Level Monitoring*: Wie wird die Erfüllung der Service Levels gemessen? Über welche Parameter wird informiert? Welches sind die Mess- und Abrechnungsperioden (Synchronisierung mit Vergütungsperioden!)? Besteht eine Möglichkeit zur externen Überprüfung?

2.5.5. *Service Level Management* (z.B. automatische Preisminderungen, Malus, Konventionalstrafen)

2.5.6. *Release Management* für Software (Beschreibung von Releasezyklus, Testing, Ablehnungsmöglichkeiten neuer Releases, Pflege von individuellen Modifikationen und Konfigurationen etc.)

2.6. Change Management

2.6.1. *Voraussetzungen für Leistungsänderungen auf Wunsch der Anwaltskanzlei* (z.B. Mindestbezugsmengen / Mindestbezugsdauern, Skalierungsmöglichkeiten, Exit-Optionen)

2.6.2. *Voraussetzungen für Leistungsänderungen auf Wunsch des Providers* (z.B. garantierte Mindestdauer bestimmter Services, Vorankündigungsfristen für die Einstellung oder Änderung bestimmter Services oder Schnittstellen, Definition von Subunternehmern, bei deren Wechsel die ausdrückliche Zustimmung der Anwaltskanzlei eingeholt werden muss)

2.6.3. Beschreibung des *Prozesses zur Anpassung der Services* an veränderte Anforderungen, insbesondere Skalierbarkeit (z.B. Storage, Bandbreiten, Softwarelizenzpakete) und Modalitäten der Skalierung (z.B. wie rasch und zu welchen Kosten die Mengen erhöht oder reduziert werden können)

3. Vergütungen

3.1. Vergütungen

3.1.1. *Pauschalpreise* (z.B. für ein bestimmtes Leistungspaket)

3.1.2. *Nutzungsabhängige Gebühren* (z.B. nach Datenvolumen / zeitlicher Beanspruchung von Rechenleistung und Applikationen). Gibt es zusätzlich auch Flatrates (z.B. bei Erreichen bestimmter Schwellenwerte)? Gibt es eine Best Price Option?

3.1.3. *Aufwandsabhängige Leistungen* (Ansätze, Anforderungsprofile etc.)

3.2. Zusätzliche Kosten

3.2.1. Überwälzung von Auslagen, Spesen und Gebühren

3.2.2. Tragung von Umsatzsteuern (anwendbare Steuern, Steuersätze etc.)

3.3. Anpassungsmöglichkeiten von Vergütungen

3.3.1. Erhöhung und Reduktion entsprechend dem effektiven *Nutzungsumfang*

3.3.2. *Mengenrabatte* (z.B. für skalierbare Leistungen)

3.3.3. Zeitlich *degressive Vergütungen* (z.B. Infrastrukturleistungen)

3.3.4. *Indexierung* (z.B. aufwandsabhängige Leistungen)

3.3.5. Kosten für die *Pflege von individuellen Softwareanpassungen*

3.3.6. Eventuell *Benchmarking* marktgängiger Leistungen (Voraussetzungen, Wirkung, Kostentragung etc.)

3.4. Messung des Leistungsbezugs

3.5. Fälligkeitstermine, Abrechnungs- und Zahlungsmodalitäten

3.5.1. *Beginn und Ende* der einzelnen Vergütungspflichten entsprechend der tatsächlichen Nutzung

3.5.2. *Abrechnungs- und Zahlungsmodalität*en (Abrechnungsperioden mit Service Level Management koordinieren!)

3.6. Verzug und Lösung von Differenzen über Zahlungsverpflichtungen

3.6.1. Folgen bei *Verzug der Anwaltskanzlei* (z.B. Verzugszinsen, Leistungseinstellung, Vertragsauflösung)

3.6.2. *Hinterlegungsmöglichkeit* auf ein Sperrkonto mit befreiender Wirkung bei Auseinandersetzungen über Zahlungspflichten, vertragliches Konflikteskalationsverfahren bezüglich der Herausgabe

3.6.3. *Verrechenbarkeit* gegenseitiger Ansprüche

3.6.4. Ausschluss der *Zurückbehaltung oder Löschung von Daten der Anwaltskanzlei*

4. Sicherheit, Geheimnis- und Datenschutz

4.1. Geheimnis- und Datenschutz

4.1.1. Definition von *Art, Zweck und Umfang der Erfassung, Bearbeitung und Nutzung von Klienten- und sonstigen Personendaten*, insbesondere Kreis der Betroffenen und der Zugriffsberechtigten, Dauer der Nutzung, Archivierung und Löschung der Daten.

4.1.2. *Compliance mit Geheimhaltungs- und Datenschutzvorschriften* seitens der Anwaltskanzlei und des Providers sowie seiner Subunternehmer (z.B. Registrierung von Datensammlungen, Bearbeitungsreglemente, Datenschutzbeauftragte). Innerhalb von internationalen Anwaltskanzleien müssen unter Umständen kumulativ die Normen mehrerer Länder eingehalten werden!

4.1.3. *Unterstellung des Providers* und seiner Subunternehmer als Hilfsperson unter die für die Anwaltskanzlei geltenden Geheimhaltungs- und Datenschutzvorschriften

4.1.4. Definition einer *Ansprechstelle* für alle Belange des Datenschutzes auf Seiten der Anwaltskanzlei sowie auf Seiten des Providers und seiner

Subunternehmer (z.B. Datenschutzverantwortlicher gemäss Art. 11a Abs. 5 lit. e DSG)

4.1.5. Unterstützungspflichten des Providers bezüglich von *Betroffenenrechten* (Auskunft, Berichtigung, Löschung und Sperrung der Daten)

4.1.6. *Geheimhaltungspflicht und Verwertungsverbot* des Providers sowie Pflicht zur Aufklärung, Überbindung und Überwachung der Einhaltung der Vorgaben auf Arbeitnehmer, Subunternehmer, Konzerngesellschaften etc., welche Einblick in die Daten der Anwaltskanzlei erhalten könnten

4.1.7. *Zertifizierungen des Providers* und seiner Subunternehmer, Verpflichtung zu deren Aufrechterhaltung

4.1.8. *Allfällige Zertifizierungen der Anwaltskanzlei,* Mitwirkungspflichten des Providers und Vergütung von Aufwand in Zusammenhang mit Zertifizierungsprozessen

4.1.9. Technische und organisatorische Massnahmen zur *Vermeidung und Erkennung* allfälliger Geheimnis- und Datenschutzverletzungen (z.B. Trennung der Daten verschiedener Kunden, Beschränkungen und automatische Protokollierung der Zugriffe)

4.1.10. *Verbot der Verlagerung der Leistungserbringung ins Ausland oder auf Subunternehmer* ohne vorgängige schriftliche Zustimmung der Anwaltskanzlei

4.1.11. Besondere Massnahmen zum Schutz von Daten, welche *den Anwaltsgeheimnis sowie allfälligen weiteren spezialgesetzlichen oder besonderen vertraglichen Geheimhaltungspflichten* unterstehen

4.1.12. Sofortige *Informationspflichten des Providers gegenüber* der Anwaltskanzlei für den Fall bestimmter Incidents, insbesondere Verstössen gegen Geheimhaltungs-, Datenschutz- oder Informationssicherheitspflichten (siehe auch Ziff. 2.3.3)

4.1.13. Regelungen über rechtlich zulässige Information der Anwaltskanzlei wenn Strafverfolgungsbehörden und andere *staatliche Stellen Informationen* verlangt oder erhalten haben; Verpflichtung des Providers zur Ausschöpfung von Rechtsbehelfen und Einreden (auch gestützt auf das Anwaltsgeheimnis) gegenüber staatlichen Herausgabebegehren; Erklärung des Providers, auf freiwillige Datenherausgabe oder freiwillige Erteilung von Zugriffsrechten auf Daten gegenüber staatlichen Organen zu verzichten

4.1.14. *Folgen* von Geheimnis- und Datenschutzverletzungen (z.B. Informationspflichten, Konventionalstrafen, ausserordentliche Kündigungsrechte)

4.2. Informationssicherheit

4.2.1. Anwendbare *Sicherheitsstandards*, Zertifizierungen

4.2.2. *Sicherheitskonzept*; Beschreibung des Prozesses und der Verantwortlichkeiten bei der Erstellung und Aktualisierung des Informationssicherheits- und Datenschutzkonzepts

4.2.3. Beschreibung der *Prozesse, Rollen und Verantwortlichkeiten* (Bestandteil des Sicherheitskonzepts)

4.2.4. *Beschreibung der Sicherheitsarchitektur* (Trennung von Entwicklungs-, Test- und Produktionssystemen, Systemredundanzen, Firewalls, Intrusion Detection Systeme etc.)

4.2.5. Beschreibung von *Verschlüsselungsmethoden* und Schlüsselmanagement für Speichermedien und für den Datenverkehr zwischen Anwaltskanzlei und Provider

4.2.6. Detaillierte Beschreibung der *Authentifizierungsprozesse* zur Nutzung des Services und der Benutzerverwaltung; Auditierbarkeit von Login-Vorgängen etc.

4.2.7. *Logging*: Definition, welche Zugriffe auf Daten und Systeme in Logfiles aufgezeichnet werden, wie und durch wen diese ausgewertet werden können

4.2.8. *Risiko- und Katastrophenvorsorge* (z.B. redundante Anbindung an Internet, Stromversorgung etc.); Beschreibung der Prozesse und der Service Levels für Back-Up und Recovery

4.2.9. Rechte und Pflichten des Providers bei massiven Sicherheitsproblemen oder im *Katastrophenfall*: Wann darf und muss der Provider selber kurzfristig welche Massnahmen treffen (mit oder ohne Einbezug der Anwaltskanzlei)?

4.2.10. Beschreibung der *Security-Checks*, die beim Provider durchgeführt werden (Audits, Penetration Tests etc.) und Wahrung der Geheimhaltungspflichten bei deren Durchführung

4.3. Datensicherung, Archivierung und Datenlöschung

4.3.1. Umfang, Art und Frequenz der *Datensicherung*

4.3.2. Compliance mit Vorschriften zur Beweissicherung und Archivierung bestimmter Daten (z.B. Anwaltsrecht, Steuerrecht, Buchführungsrecht, Sozialversicherungsrecht); Definition der betroffenen Prozesse und Daten, Art, Umfang und Dauer der *Archivierung*, Rückübermittlungsprozess an die Anwaltskanzlei, Prüfungs- und Kontrollrechte

4.3.3. *Aufbewahrung von Sicherungsmedien* (räumliche Trennung, Kennzeichnung, Verschlüsselung der Sicherungen, Zugriffsmöglichkeiten der Anwaltskanzlei etc.)

4.3.4. *Verwertungsverbot* und Verzicht auf allfällige Retentionsrechte an Daten der Anwaltskanzlei (insbesondere für den Fall eines Zahlungsverzuges der Anwaltskanzlei oder der Insolvenz des Providers)

4.3.5. *Verfahren der Datenlöschung*

4.4. Audit und Kontrollrechte

4.4.1. *Audit- und Kontrollrechte* beim Provider und seinen Subunternehmern

4.4.2. *Mitwirkungspflichten des Providers* bei Audits und Kontrollen

4.4.3. Beizug von *Drittexperten* zur Durchführung der Audits und Kontrollen im Auftrag der Anwaltskanzlei (insbesondere Verfahren zu deren Bestimmung)

4.4.4. *Eigene Auditierungspflichten des Providers* (z.B. im Rahmen von Zertifizierungen oder behördlichen Kontrollen); Welche Informationen daraus werden der Anwaltskanzlei zur Verfügung gestellt?

4.4.5. Einbindung in ein allfälliges *Interne Kontrollsystem* der Anwaltskanzlei

4.4.6. Kontrollrechte von *Aufsichtsbehörden der Anwaltskanzlei* (z.B. Anwaltsaufsichtsbehörde, ESTV, EDÖB) beim Provider und seinen Subunternehmern

4.4.7. Tragung von *Kosten und Aufwand* in Zusammenhang mit Audits und Kontrollen

5. Gewährleistung und Haftung

5.1. Abgrenzung der Risikosphären zwischen Anwaltskanzlei und Provider sowie Dritten (z.B. Zugangsprovidern)

5.2. Haftung

5.2.1. Beweis und Berechnung von Schäden

5.2.2. Bedeutung des Verschuldens im Hinblick auf Haftungsansprüche

5.2.3. Haftungsausschlüsse

5.2.4. Verhältnis zu allfälligen Konventionalstrafen

5.2.5. Verjährungsfristen

5.3. Rechtsgewährleistung

5.4. Versicherung von Risiken durch den Provider

6. Vertragsdauer und Vertragsbeendigung

6.1. Vertragsdauer

6.1.1. *Inkrafttreten* des Vertrages

6.1.2. *Vertragsdauer*

6.2. Ordentliche Kündigungsmöglichkeiten

6.2.1. Kündigungsfristen

6.2.2. Kündigungstermine

6.2.3. Form

6.3. Ausserordentliche Vertragsauflösungsmöglichkeiten

6.3.1. Ausserordentliche Vertragsauflösungsgründe

6.3.2. Kündigungsfristen

6.3.3. Form

6.4. Folgen der Vertragsauflösung

6.4.1. *Vergütung* (Berechnung für angebrochene Perioden *pro rata temporis*)

6.4.2. Schutz der Daten der Anwaltskanzlei und der Verfügbarkeit der Anwendungen bei *Insolvenz des Providers* (z.B. Kennzeichnung von Datenträgern im Hinblick auf eine Aussonderung, Verwertungsverbot für Daten, Herausgabe von Datensicherungen und Dokumentationen, Escrow des Sourcecodes von Software)

6.4.3. Beschreibung der *Prozesse bei Vertragsbeendigung* (z.B. Zugangsbeendigung, Auslieferung und Löschung von Daten, Übergabe elektronischer Schlüssel, Abrechnungsmodalitäten)

6.5. Backsourcing

6.5.1. *Unterstützungspflichten* des Providers (z.B. Datenmigration)

6.5.2. *Planung des Vorgehens* (Backsourcingkonzept, Datenmigration, Verantwortlichkeiten etc.)

6.5.3. *Lieferung* von Daten, Dokumentationen, Schnittstelleinformationen, Parametrisierungsinformationen, virtuelle Maschinen etc.

6.5.4. *Konditionen einer Weiterführung der Services* während einer Übergangsphase

6.5.5. *Vergütung* von Unterstützungsleistungen

7. Weitere Bestimmungen

7.1. Recht und Gerichtsstand

7.1.1. Anwendbares Recht

7.1.2. Gerichtsstand, eventuell vertragliches Konflikteskalationsverfahren / alternatives Streitbeilegungsverfahren

7.2. Schlussbestimmungen

7.2.1. *Rechtsnachfolge*, eventuell grundsätzliche Zustimmung zur Übertragung des Vertrages unter Vorbehalt bestimmter Ablehnungsgründe → Ablehnungsverfahren definieren

7.2.2. *Offenlegung*: Recht der Anwaltskanzlei, die Bedingungen des Vertrages gegenüber ihren Aufsichtsbehörden und dem EDÖB offen zu legen

7.2.3. *Schriftform/Formvorbehalte*

7.2.4. *Unterschriften* → darauf achten, dass die Unterzeichnenden unterschriftsberechtigt sind (z.B. aktuellen Handelsregisterauszug als Anhang aufnehmen)

WOLFANG STRAUB, Dr. iur., LL.M., Fürsprecher, ist Rechtsanwalt in Bern und Lehrbeauftragter am CAS ICT Beschaffungen der Universität Bern

Die vorliegende Checkliste ist aus der Diskussion mit zahlreichen Kolleginnen und Kollegen heraus entstanden. Für wertvolle Anregungen und Hinweise danke ich namentlich CHRISTIAN LAUX und PETER NEUENSCHWANDER.