SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

SAV-Wegleitung für IT-Outsourcing und Cloud-Computing

I. Einleitung

1 Eine funktionierende IT-Infrastruktur ist bereits heute systemkritisches Element in der Organisation von Anwaltskanzleien. Die Bedeutung von Technologie in der Anwaltsbranche wird sich jedoch in den kommenden Jahren mit der zunehmenden Digitalisierung der Arbeitsabläufe, der Dezentralisierung von Arbeitsorten (Home-Office) sowie der Verbreitung neuer softwarebasierter Hilfsmittel (LegalTech) nochmals verstärken. Von dieser Entwicklung werden vermehrt auch kleinere Kanzleistrukturen betroffen sein.

2 Um einen sicheren und kosteneffizienten Betrieb der eingesetzten Hard- und Software sicherstellen zu können, werden viele Anwälte externe Anbieter beiziehen müssen (IT-Outsourcing), welche als Hilfspersonen ihre Dienstleistungen im Zusammenhang mit der Datenspeicherung und -bearbeitung sowie der Organisation des Datenzugriffs vielfach über das Internet erbringen (Cloud-Computing).

3 Die herrschende Lehre[1] und Rechtsprechung[2] anerkennen, dass der Beizug von externen IT-Dienstleitungsprovidern nicht in einem grundsätzlichen Widerspruch zum Berufsgeheimnis von Anwältinnen und Anwälten steht. Auch der Schweizerische Anwaltsverband (SAV) stellt fest, dass IT-Outsourcing und Cloud-Computing sich in allen Industrie- und Dienstleistungssparten zum Standard entwickelt haben und auch für Anwaltskanzleien nicht mehr wegzudenkende Vorteile mit sich bringen. Dazu gehören insbesondere:

- Erhöhte physische Sicherheit der Hardware und erhöhte Datensicherheit durch Professionalisierung des IT-Infrastrukturbetriebs.
- Kostenersparnisse in Bezug auf Hardware und IT-Mitarbeiter.
- Ausbau der Funktionalität und Zuverlässigkeit der IT-Infrastruktur.
- Vereinfachung des Zugriffs auf die IT-Infrastruktur.

4 Mit IT-Outsourcing und Cloud-Computing geht indes stets ein Verlust der (vermeintlich) absoluten Daten- und Systemkontrolle einher, was potenziell neue Risiken birgt. Zu diesen gehören:

- Risiken im Zusammenhang mit der Einhaltung anwaltlicher Berufspflichten, insbesondere des Berufsgeheimnisses.
- Risiken im Zusammenhang mit datenschutzrechtlichen Vorgaben.
- Vertragliche und systembedingte Risiken im Zusammenhang mit Outsourcing Verträgen (Kontrolle über die Daten und deren Speicherort, Beizug von Sublieferanten durch Hilfspersonen, Kontrolle über Sicherheit der Daten, Sicherstellung des Zugriffs auf Daten).

5 Es stellt sich vor diesem Hintergrund die Frage, unter welchen Voraussetzungen und Schranken eine Anwaltskanzlei ihre IT auslagern und Cloud-Computing-Dienstleistungen in Anspruch nehmen darf, damit die digitalen Arbeitsabläufe mit den Berufsregeln, insbesondere dem Anwaltsgeheimnis und den übrigen gesetzlichen (z.B. datenschutzrechtlichen) Vorgaben vereinbar sind.

6 Der SAV veröffentlicht die vorliegende, überarbeitete Wegleitung mit dem Ziel, technologie- und risikogerechte Verhaltensgrundsätze für IT-Outsourcing und den Einsatz von Cloud-Computing-Dienstleistungen als Branchenstandard zu schaffen (*Best Practice*). Es geht dem SAV nicht darum, in der vorliegenden Wegleitung die in Literatur und Rechtsprechung zu diesem Thema erfolgte Diskussion inhaltlich zusammenzufassen. Vielmehr stellt die Wegleitung das auf die praktische Anwendung hin konzipierte Kondensat der Auseinandersetzung des SAV mit diesem Thema dar. Mit dem praxisorientierten Fokus soll die Rechtssicherheit gestärkt und den Anwältinnen und Anwälten ermöglicht werden,

---

1 So Yaniv Benhamou / Frédéric Erard / Daniel E. Kraus, L'avocat a-t-il aussi le droit d'être dans les nuages? Revue de l'avocat, 2019, vol. 22, n° 3, p. 119-12; Benoît Chappuis / Adrien Alberini, Secret professionnel de l'avocat et solutions cloud, Revue de l'avocat 8/2017, p. 337, 338; Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 1/2019, S. 28 f.; vgl. auch David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020.

2 Vgl. BGE vom 4. Juni 2019, 2C 1083/2017.

auch im Zuge der fortschreitenden Digitalisierung weiterhin konkurrenzfähige, zuverlässige und qualitativ hochstehende Dienstleistungen unter Wahrung der rechtlichen Rahmenbedingungen zu erbringen.

7 Diese Wegleitung enthält Empfehlungen, die das SAV-Mitglied bei der Beschaffung und beim Einsatz von Cloud-Dienstleistungen als Hilfestellung heranziehen kann. Sie zeigt die rechtlichen Rahmenbedingungen auf und beinhaltet auch Auslegungen bestehender Normen, um damit Rechtsunsicherheiten aufgrund fehlender Rechtsprechung für die zum Teil neuartigen Herausforderungen beim Einsatz von Cloud-Dienstleistungen zu beheben. Es bleibt jedoch wichtig, dass die Anwaltskanzleien bei der Anwendung dieser Wegleitung ihre konkreten Bedürfnisse risikobasiert und -adäquat berücksichtigen.

II. Definitionen

- **IT-Outsourcing**: Outsourcing bzw. Auslagerung von Unternehmensaufgaben und -strukturen im Bereich IT an externe Dienstleister.
- **Cloud-Computing:** Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung durch technische Schnittstellen und Protokolle über das Internet. Die eigentliche IT-Infrastruktur wird dabei nicht mehr auf lokalen Servern, sondern extern bei einem Cloud-Anbieter bereitgestellt und über das Internet genutzt. Es existieren viele, sehr unterschiedliche Angebote, wobei der physische Standort der Daten und Schutzmassnahmen wie Verschlüsselung von Bedeutung sind.
- **IT-Dienstleister**: Dienstleister, welcher von einer Anwältin oder einem Anwalt als Hilfsperson für die Erfüllung von Cloud-Computing oder anderen IT-Outsourcing Aufgaben beigezogen wird.

III. Wegleitung

8 Die Anwältin oder der Anwalt hat die IT-Infrastruktur einer Anwaltskanzlei und den Beizug von IT-Dienstleistern in einer Weise sicherzustellen, dass die auf ihn anwendbaren regulatorischen und gesetzlichen Vorgaben eingehalten werden. Dazu gehören insbesondere die Pflicht zur sorgfältigen Berufsausübung,[3] das Berufsgeheimnis der Anwältinnen und Anwälte[4] sowie weitere gesetzliche Vorgaben wie z.B. das Datenschutzrecht. Zu diesem Zweck müssen sich die Anwältinnen und Anwälte ihrerseits durch Sorgfalt bei der Wahl der IT-Infrastruktur sowie bei der Auswahl, Instruktion und Überwachung des IT-Dienstleisters leiten lassen.

A. Beizug IT-Dienstleister

1. Welche Kriterien sind bei der Wahl eines IT-Dienstleisters zu beachten?

9 Der IT-Dienstleister wird zu einem systemkritischen Element in der Organisation der Anwaltskanzlei. Entsprechend ist es die Pflicht der Anwältin und des Anwalts, den IT-Dienstleister vor dessen Auswahl einer sorgfältigen Prüfung zu unterziehen und dabei

3 Art. 12 lit. a BGFA.

4 Art. 13 BGFA; Art. 321 StGB.

insbesondere zu prüfen, ob der IT-Dienstleister die ihm zu übertragenden Aufgaben mit der gebotenen Sorgfalt und Professionalität wahrnehmen kann. Dabei sind insbesondere folgende Kriterien relevant:

- Fähigkeit zur vertragskonformen Erfüllung der übertragenen Aufgaben.
- Erfahrung und Ruf des IT-Dienstleisters.
- Domizil und Standort des IT-Dienstleisters.
- Referenzkunden im Anwalts- oder in verwandten Dienstleistungsmärkten (z.B. Anzahl Kanzleien oder sonstige Berufsgeheimnisträger, welche Grösse, in welchen Ländern).
- Finanzielle Situation des IT-Dienstleisters (wirtschaftliche Stabilität, Zahlungsfähigkeit, Zuverlässigkeit, Eigentümerschaft und Kapitaladäquanz).
- Anzahl Mitarbeiter, welche für die IT-Dienstleistung zuständig sind (Support und Entwickler).
- Abhängigkeit von Zulieferern.
- Transparenzberichterstattung des IT-Dienstleisters (bezüglich etwaigen Anfragen auf Datenherausgaben von in- und/oder ausländischen Behörden oder Angriffe auf Server-/Rechenzentrumsinfrastrukturen etc.)
- Zukunftsperspektive für die Weiterentwicklung der anvisierten Lösung.
- Genaue Lokalisierung der Speicherserver (insb. im Ausland).
- Physische und elektronische Sicherheit der Server sowie des Rechenzentrums, in dem die Server sich befinden.
- Falls Unternehmen, Konzerngesellschaft oder anderweitige Präsenz im Ausland oder (andere) Zugriffsmöglichkeiten aus dem Ausland auf Daten in der Schweiz: Prüfung der anwendbaren zivilrechtlichen, strafrechtlichen und anderen Vorschriften, insb. in Bezug auf Herausgabe von Klientendaten (z.B. CLOUD Act der USA) unter Berücksichtigung der Wahrscheinlichkeit eines Datenzugriffs aufgrund des konkreten Risikoprofils der bei einer Anwältin oder einem Anwalt vorhandenen Klientendaten (Natur der Daten).

10 Die Auswahl des IT-Dienstleisters hat somit unter Berücksichtigung und Prüfung von dessen professionellen Fähigkeiten sowie finanziellen und personellen Ressourcen zu erfolgen. Dabei hat sich die Wahl an den konkreten Datensicherheits- und Infrastrukturbedürfnissen der Kanzlei, resp. der mit der Aufbewahrung der konkreten Klientendaten verbundenen faktischen, rechtlichen und wirtschaftlichen Risiken, zu orientieren. Der IT-Dienstleister muss sicherstellen können, dass die gewählte IT-Infrastruktur sowie deren Betrieb in technischer und organisatorischer Hinsicht das Niveau an Datensicherheit, Verwendungskontrolle, Integrität und Verfügbarkeit gewährleistet, welches für die entsprechende Kanzlei und deren Klienten erforderlich ist. Auch sind im Lichte von Art. 211 SchKG die nötigen Vorkehren für den Insolvenzfall des IT-Dienstleisters zu treffen: Die Verträge sind so auszugestalten, dass bei einem Konkurs die Kontinuität des Zugriffs auf die Daten sichergestellt bleibt bzw. auf einen anderen IT-Provider übertragen werden kann oder eine sogenannte Failover-Infrastruktur (operativer Backup Modus) aufgebaut ist.

11 Werden mehrere Funktionen an den gleichen IT-Dienstleister ausgelagert, ist zudem dem Konzentrationsrisiko Rechnung zu tragen.

2. Was ist bei der Ausgestaltung des IT-Dienstleistungsvertrags zu beachten?

12 Der Beizug des IT-Dienstleisters muss auf einem schriftlichen Vertrag beruhen. Der SAV empfiehlt, einen der durch den SAV ausgearbeiteten Musterverträge[5] zu verwenden oder als Leitfaden bei den Vertragsverhandlungen beizuziehen.

13 Für die Anwältin und den Anwalt im Vertragsverhältnis mit dem IT-Dienstleister wichtige Punkte sind insbesondere:

- *Beizug Subunternehmer:* Der Beizug von Subunternehmern durch den IT-Dienstleister muss vertraglich eingeschränkt sein. Dürfen Subunternehmer beigezogen werden, so sind diese namentlich aufzuführen. Auch sind ihnen die Pflichten und Zusicherungen des IT-Dienstleisters zu überbinden und die Anwältin oder der Anwalt muss (direkt oder indirekt über die Hilfsperson) auch gegenüber den Subunternehmern ein Weisungsrecht haben. Vor dem Hintergrund der aktuellen Bundesgerichtspraxis[6] wird jedoch empfohlen sicherzustellen, dass Subunternehmer – sollten sich diese nicht direkt gegenüber der Anwältin oder dem Anwalt zur Geheimhaltung verpflichten – keine Einsicht in dem Anwaltsgeheimnis unterstellte Daten haben. Dies kann z.B. mittels Verschlüsselung der Daten erreicht werden.
- *Klarheit über Ort der Datenbearbeitung bzw. -speicherung:* Der Vertrag schafft Klarheit, von wo aus der IT-Dienstleister seine Leistungen erbringt, von wo er auf die Daten zugreift und wo die Daten gespeichert werden.
- *Geheimhaltungspflicht:* Die Wahrung des Berufsgeheimnisses durch den IT-Dienstleister (und allfällige Subunternehmer) ist vertraglich abzusichern. Der IT-Dienstleister ist darauf hinzuweisen, dass er als Hilfsperson dem Berufsgeheimnis (Art. 321 StGB; Art. 13 BGFA) unterliegt. Er ist vertraglich zur Geheimhaltung zu verpflichten. Zudem ist er zu verpflichten, seine Pflichten und Zusicherungen gegenüber der Anwältin oder dem Anwalt auch allfälligen, im Vertrag aufgeführten Subunternehmern zu überbinden und sicherzustellen, dass entweder die Anwältin oder der Anwalt selbst oder der IT-Dienstleister gegenüber dem Subunternehmer weisungsbefugt ist.
- *Datenschutz:* Sicherstellung, dass die Vorgaben des anwendbaren Datenschutzrechts eingehalten werden.
- *Umgang mit und Herausgabe von Daten:* Klarstellung, dass die rechtliche Herrschaft über die Daten jederzeit bei der Anwältin und dem Anwalt verbleibt und diese auf Verlangen an die Anwältin und den Anwalt herausgegeben werden müssen. Regelung der Beziehung im Falle des Konkurses des IT-Dienstleister (Business-Continuity), der Vertragsbeendigung, der Rückführbarkeit und Rückführungsmodalität der Daten wie auch der Pflichten des IT-Dienstleisters in Zusammenhang mit Herausgabebegehren Dritter (Lawful Access).

---

5 https://digital.sav-fsa.ch/digitale-kanzlei-cloud-und-datenschutz

6 Vgl. BGE vom 4. Juni 2019, 2C 1083/2017.

- *Zugriff auf Daten:* Klarstellung, wann, von wo und zu welchem Zweck der IT-Dienstleister auf Daten zugreifen kann und welche Mitarbeiter des IT-Dienstleisters (und allfälliger Subunternehmer) auf Daten zugreifen können.
- *Datensicherheit:* Regelung des sicherheitstechnischen Schutzniveaus der Daten bei Übermittlung, Bearbeitung und Speicherung. Regelung der Informationspflichten des IT-Dienstleisters, falls Sicherheitslücken entdeckt oder von Dritten ausgenutzt wurden.
- *Service Level Agreement (SLA):* Klare Spezifizierung der zu erbringenden Dienstleistungen und von deren Verfügbarkeit sowie Qualität. Die Zuständigkeiten des Nutzers und des Dienstleisters sind vertraglich festzulegen und abzugrenzen, insbesondere bezüglich Schnittstellen und Verantwortlichkeiten.
- *Backup / Disaster-Recovery / Contingencies*: Der Vertrag enthält ein Sicherheitsdispositiv, das die schnelle Weiterführung der ausgelagerten Funktion, insbesondere den schnellen Zugriff auf die Daten in Notfällen erlaubt (Backup der Daten, Zugriff auf Backup, alternative Internetverbindungen).
- *Weisungs- und Kontrollrechte:* Die Anwältin und der Anwalt haben sich die Weisungs- und Kontrollrechte gegenüber dem IT-Dienstleister (und direkt oder indirekt gegenüber dessen Subunternehmern) vertraglich zusichern zu lassen. Sie/er hat das Recht, die Dienstleistungen und die Infrastruktur des IT-Dienstleisters (und gegebenenfalls von dessen Subunternehmern) einem Audit hinsichtlich Datensicherheit und Einhaltung der vertraglichen Vorgaben (z.B. Geheimhaltungspflicht, Datenschutzrecht) zu unterziehen, respektive unterziehen zu lassen.
- *Vertragsdauer:* Sicherstellung, dass im Falle einer Vertragskündigung durch den IT-Dienstleister die Anwältin und der Anwalt ausreichend Zeit zur Eruierung von Ersatzlösungen haben.
- *Unterstützungspflichten IT-Dienstleister bei Vertragsende*: Regelung der Pflichten des IT-Dienstleisters, um den Wechsel der Anwältin und des Anwalts zu einem anderen Dienstleister zu ermöglichen, respektive zu unterstützen (Anforderungen an Einhaltung Standards, Migrationsunterstützung etc.). Die geordnete Rückführung der ausgelagerten Funktion muss sichergestellt sein.

3. Wie ist der IT-Dienstleister zu überwachen?

14 Die Einhaltung der Kernverpflichtungen eines IT-Dienstleisters (Wahrung des Berufsgeheimnisses und Verwendung der Daten nur zur Vertragserfüllung) sind in zumutbarer Weise risikobasiert zu überwachen.[7]

15 Bei überschaubaren Kanzleigrössen mit geringem Risikoprofil (Natur der Daten) genügt es in diesem Zusammenhang grundsätzlich, einen unabhängigen Spezialisten zu beauftragen, das Sicherheitsdispositiv des Cloud-Providers zu prüfen. Es kann aber auch auf ein zertifiziertes Qualitätsmanagementsystem des IT-Dienstleisters nach ISO 9001 bzw. 27001 oder auf eine datenschutzspezifische Zertifizierung (z.B. GoodPriv@cy, VDSZ:2014 oder ePrivacy) abgestellt werden.

7 Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, a.a.O., S. 32.

16 Unabhängig davon empfiehlt es sich bei jeder Kanzleigrösse, eigenständige Massnahmen zu treffen, wie z.B.:

- Regelmässiges Testen des Zugriffs auf Backups und von Disaster Recovery Szenarien.
- Regelmässige Prüfung der Aktualität von Antivirensoftware.

17 Je nach Grösse und Tätigkeit der Kanzlei kann aber auch ein eigenes Sicherheitsdispositiv erforderlich sein. Die an den IT-Dienstleister ausgelagerte Funktion ist diesfalls in das interne IT-Kontrollsystem / Sicherheitsdispositiv der Kanzlei zu integrieren. Dieses ist dem Datenrisikoprofil der Anwaltskanzlei entsprechend auszugestalten. Dabei haben die Anwältin und der Anwalt die mit dem Betrieb ihrer IT-Infrastruktur sowie die mit der Auslagerung verbundenen wesentlichen Risiken systematisch zu identifizieren, zu überwachen, zu quantifizieren und zu steuern. Bei besonders sensiblen Informationen sind angemessene technische und organisatorische Massnahmen zum Schutz solcher Informationen zu ergreifen. Die Beachtung der zivil- und berufsrechtlichen Pflichten erfordert eine sinnvolle Begrenzung des Personenkreises mit Zugang zu Klientendaten.

B. Information des Klienten

1. Muss der Klient über den Beizug eines IT-Dienstleisters informiert werden?

18 Der Beizug eines IT-Dienstleisters ist sowohl aus Perspektive des Anwaltsrechts wie auch des geltenden Datenschutzrechts auch ohne vorgängige Einwilligung des Klienten zulässig. Mit dem künftigen DSG wird indes eine generelle Informationspflicht eingeführt.

19 Im Sinne der Transparenz empfiehlt es sich jedoch bereits heute, die Klienten in Mandatsverträgen oder Vollmachten über die Nutzung von IT-Outsourcing und elektronischen Kommunikationsmitteln zu informieren. Damit kann gleichzeitig die Einwilligung der Klienten eingeholt werden. Diese kann auch formlos und konkludent erteilt werden – beispielsweise indem die Verwendung solcher IT-Dienstleistungen oder Kommunikationsmittel von den Klienten initiiert wurde.

20 Soweit die Anwältin oder der Anwalt im Rahmen der Klientenbeziehung bestimmte IT-Dienstleistungen sowie elektronische Kommunikationsmittel einsetzt (z.B. Skype, Email, Google-Docs, Office 365, Bearbeitung von Daten im Ausland etc.), ist der Klient in der Mandatsvereinbarung in allgemeiner Weise auf Datensicherheitsrisiken hinzuweisen. Falls die Verwendung einer IT-Dienstleistung oder eines Kommunikationsmittels durch den Klienten initiiert wurde, entfällt diese Obliegenheit.

2. Formulierungsvorschlag des SAV für die Mandatsvereinbarung

Der SAV empfiehlt folgende oder eine vergleichbare Regelung im Mandatsvertrag zwischen Kanzlei und Klient aufzunehmen:

"*Wir weisen Sie darauf hin, dass wir im Rahmen der Erbringung unserer Dienstleistungen auf externe IT-Dienstleister und Cloud-Provider mit Servern in der Schweiz [oder im*

Ausland][8] zurückgreifen und bestimmte IT-Dienstleistungen sowie Kommunikationsmittel einsetzen, welche mit Datensicherheitsrisiken verbunden sein können (z.B. Email, [Skype, Google Docs, DropBox] etc.). Wünschen Sie für Ihre Daten besondere Sicherheitsmassnahmen, so obliegt es Ihnen, uns darüber zu orientieren."

Vorstandsbeschluss vom 11. November 2022.

8 Es ist weiter sicherzustellen, dass im Mandatsvertrag die notwendigen datenschutzrechtlichen Bestimmungen enthalten sind.