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 einer Anwaltskanzlei. Die Bedeutung der IT wird sich jedoch in den kommenden Jahren mit der zunehmenden Digitalisierung der Arbeitsabläufe in der Anwaltsbranche nochmals verstärken. Um einen sicheren und kosteneffizienten Betrieb der eingesetzten Hard- und Software sicherstellen zu können, werden viele Anwälte professionelle externe Anbieter beiziehen müssen (IT-Outsourcing), welche ihre Dienstleistungen im Zusammenhang mit der Datenbearbeitung und -speicherung sowie der Organisation des Datenzugriffs als Hilfsperson vielfach über das Internet erbringen (Cloud-Computing).

2 Nach der herrschenden Lehre gelten Cloud-Provider als Hilfspersonen von Anwältinnen und Anwälten[1]. Auch der Schweizerische Anwaltsverband (SAV) anerkennt, dass Cloud-Computing und IT-Outsourcing sich in allen Industrie- und Dienstleistungssparten zum Standard entwickelt haben und auch für Anwaltskanzleien nicht mehr wegzudenkende Vorteile mit sich bringen können. Dazu gehören insbesondere:

- Erhöhte physische Sicherheit der Hardware und erhöhte Datensicherheit durch Professionalisierung des IT-Infrastrukturbetriebs.
- Kostenersparnisse in Bezug auf Hardware und IT-Mitarbeiter.

[1] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 1/2019, S. 28 f.

- Ausbau der Funktionalität und Zuverlässigkeit der IT-Infrastruktur.
- Vereinfachung des Zugriffs auf die IT-Infrastruktur.

3 Mit IT-Outsourcing und Cloud-Computing geht 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).

4 Mit Unsicherheit verbunden bleibt daher die Frage, unter welchen Voraussetzungen und Schranken eine Anwaltskanzlei ihre IT auslagern und Cloud-Computing-Dienstleistungen in Anspruch nehmen darf, damit diesen Risiken adäquat begegnet werden kann. D.h. wie die Anwältin sicherstellen, dass ihre digitalen Arbeitsabläufe mit den Berufsregeln, insbesondere dem Anwaltsgeheimnis und den übrigen gesetzlichen (z.B. datenschutzrechtlichen) Vorgaben vereinbar sind.

5 Der SAV veröffentlicht die vorliegende Wegleitung mit dem Ziel, technologie- und risikogerechte Verhaltensgrundsätze für IT-Outsourcing und den Einsatz von Cloud-Computing-Dienstleistungen als Branchenstandard zu schaffen (*Best Practice*). Dadurch soll die Rechtssicherheit gestärkt und den Anwälten ermöglicht werden, im Rahmen der Digitalisierung weiterhin konkurrenzfähige, zuverlässige und qualitativ hochstehende Dienstleistungen unter Wahrung der rechtlichen Rahmenbedingungen zu erbringen.

6 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, welche Rechtsunsicherheiten oder fehlende Rechtsprechung für die zum Teil neuartigen Herausforderungen beim Einsatz von Cloud-Dienstleistungen schliessen sollen. Es bleibt wichtig, dass die Anwaltskanzleien bei der Anwendung dieser Wegleitung ihre konkreten Bedürfnisse risikobasiert und verhältnismässig berücksichtigen.

## II. Definitionen

- **IT-Outsourcing**: Outsourcing bzw. Auslagerung von Unternehmensaufgaben und -strukturen im Bereich IT an externe Dienstleister. Cloud-Computing ist eine Form von IT-Outsourcing.

- **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. Die Art der Cloud unterscheidet sich je nach Art der Bereitstellung (z.B. Private Cloud, Public Cloud sowie der Art der Verschlüsselung).
- **IT-Dienstleister**: Dienstleister, welcher von einem Anwalt als Hilfsperson für die Erfüllung von IT-Outsourcing oder Cloud-Computing Aufgaben beigezogen wird.

## III. Wegleitung

7 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,[2] das Berufsgeheimnis der Anwältinnen und Anwälte[3] 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. Sorgfältige Auswahl des IT-Dienstleisters

8 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 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 Vertragserfüllung.
- Erfahrung und der Ruf des IT-Dienstleisters.
- Domizil und Standort des IT-Dienstleisters.
- Referenzkunden im Anwalts- oder verwandten Dienstleistungsmarkt (z.B. Anzahl Kanzleien oder sonstige Berufsgeheimnisträger, welche Grösse, in welchen Ländern).

---

2 Art. 12 lit. a BGFA.

3 Art. 13 BGFA; Art. 321 StGB.

- 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 Zulieferer.
- Transparenzberichte 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. Ausland).
- Physische und elektronische Sicherheit der Server sowie des Rechenzentrums, in dem die Server sich befinden.
- Falls Unternehmen, Konzerngesellschaft oder anderweitige Präsenz im oder Zugriff auf Daten aus dem Ausland: Prüfung der anwendbaren zivilrechtlichen, strafrechtlichen und anderen Vorschriften, insb. in Bezug auf Herausgabe von Klientendaten (z.B. US Cloud Act).

9 Die Auswahl des IT-Dienstleisters hat unter Berücksichtigung und Prüfung seiner professionellen Fähigkeiten sowie finanziellen und personellen Ressourcen zu erfolgen. Dabei hat sich die Wahl an den konkreten IT-Infrastrukturbedürfnissen der Kanzlei zu orientieren. Der IT-Dienstleister muss sicherstellen können, dass die gewählte IT-Infrastruktur sowie deren Betrieb den mit der Aufbewahrung der Klientendaten verbundenen faktischen, rechtlichen und wirtschaftlichen Risiken gerecht wird. Insbesondere 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 aufgebaut ist.

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

## 2. Sorgfältige Ausgestaltung des IT-Dienstleistungsvertrags

11 Der Beizug des IT-Dienstleisters muss auf einem schriftlichen Vertrag beruhen. Der SAV empfiehlt, einen der durch den SAV ausgearbeiteten Musterverträge[4] einzusetzen oder als Leitfaden bei den Vertragsverhandlungen beizuziehen.

[4] https://www.sav-fsa.ch/de/service/anwaeltin-anwalt-in-der-cloud.html

12 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.
- *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 der Anwältin gespeichert werden dürfen.
- *Geheimhaltungspflicht:* Die Wahrung des Berufsgeheimnisses durch den IT-Dienstleister ist vertraglich abzusichern. Der IT-Dienstleister ist darauf hinzuweisen, dass er als Hilfsperson dem Berufsgeheimnis (321 StGB/13 BGFA) unterliegt. Er ist vertraglich zur Geheimhaltung zu verpflichten.
- *Datenschutz:* Sicherstellung, dass die Vorgaben des anwendbaren Datenschutzrechts eingehalten werden.
- *Umgang mit und Herausgabe von Daten:* Klarstellung, dass Herrschaft über die Daten jederzeit beim Anwalt verbleibt und diese auf Verlangen an den Anwalt herausgegeben werden müssen. Regelung der Beziehung im Falle des Konkurses des IT-Dienstleister, der Vertragsbeendigung wie auch der Pflichten des IT-Dienstleisters in Zusammenhang mit Herausgabebegehren Dritter.
- *Zugriff auf Daten:* Klarstellung, wann, von wo, zu welchem Zweck 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 vertraglich zusichern zu lassen. Sie/er hat das Recht, die Dienstleistungen und die Infrastruktur des IT-Dienstleisters 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 hat.
- *Unterstützungspflichten IT-Dienstleister bei Vertragsende*: Regelung der Pflichten des IT-Dienstleisters, um den Wechsel 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. Überwachung des IT-Dienstleisters

13 Die Einhaltung der Kernverpflichtungen eines IT-Dienstleisters (Wahrung des Berufsgeheimnisses und Verwendung der Daten nur zur Vertragserfüllung) sind in zumutbarer Weise risikobasiert zu überwachen.[5]

14 Bei überschaubaren Kanzleigrössen 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) vertraut werden.[6]

15 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.

16 Je nach Grösse und Tätigkeit der Kanzlei kann aber auch ein eigenes Sicherheitsdispositiv erforderlich sein.[7] 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 hat der Anwalt die mit dem Betrieb seiner 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 der Informationen zu ergreifen. Die Beachtung

[5] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, a.a.O., S. 32
[6] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, a.a.O., S. 31
[7] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, a.a.O., S. 29

der zivil- und berufsrechtlichen Pflichten erfordert eine sinnvolle Begrenzung des Personenkreises mit Zugang zu Klientendaten. Dazu sind ausreichende Massnahmen zu deren Absicherung zu ergreifen.[8]

## B. Information des Klienten

17 Der Beizug eines IT-Dienstleisters ist sowohl aus Perspektive des Anwaltsrechts wie auch des Datenschutzrechts auch ohne vorgängige Einwilligung des Klienten zulässig.

18 Zur Absicherung und im Sinne der Transparenz empfiehlt es sich indes, 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.

19 Soweit die Anwältin 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 solchen IT-Dienstleistung durch den Klienten initiiert wurde, entfällt diese Obliegenheit.

Formulierungsvorschlag für die Mandatsvereinbarung: "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] 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."

SAV Fachgruppe Digitalisierung, Juni 2019

[8] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, a.a.O., S. 29