Sichere Cloud?


© PHH Rechtsanwälte

Gerade für Anwälte müssen die IT-Voraussetzungen stimmen

Text: Mathias Preuschl | preuschl@phh.at

Zum Autor

Mathias Preuschl ist Rechtsanwalt und Partner bei PHH Rechtsanwälte. Er ist in den Bereichen Straf- und Prozessrecht mit den Schwerpunkten Wirtschaftsstrafrecht, Zivilrecht und Compliance tätig. Darüber hinaus ist er Mitglied des Ausschusses der RAK Wien und Vorsitzender des Arbeitskreises IT des ÖRAK.

Als der veränderungsfreudigste und technologieaffinste Berufsstand gilt die Rechtsanwaltschaft nicht gerade – zu Unrecht! Denn die österreichische Anwaltschaft führt seit fast zwanzig Jahren mittels des Elektronischen Rechtsverkehrs (ERV) Verfahren. In Zeiten, in denen E-Mail als antiquiert gilt und Kommunikation via Social Media-Kanäle stattfindet, klingt das zwar nicht eben futuristisch. Doch der ERV ist in dieser Form einzigartig in Europa. Neben seinem praktischen Nutzen hat er aber auch eine psychologische und technologische Folge: Die Anwaltschaft verfügt über einen IT-Mindeststandard und ist aufgeschlossen für den IT-Einsatz in ihrer Arbeitswirklichkeit. Aber ist sie auch bereit für neuere Lösungen, wie etwa Clouds?

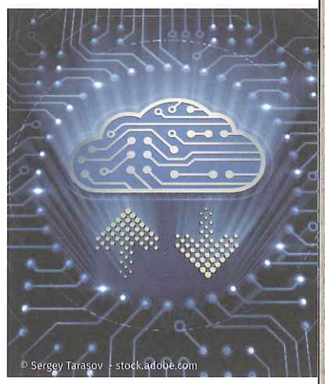
Angst vor der Cloud

Im Privaten sind Clouds kaum mehr wegzudenken und natürlich nutzen auch Österreichs Anwälte diese Möglichkeiten gern. Cloud-Lösungen auch in beruflichen Belangen einzusetzen, erzeugt bei der Anwaltschaft hingegen Irritation, um nicht zu sagen: Angst. Die Gründe für dieses Auseinanderklaffen der Akzeptanz von privater und beruflicher IT-Nutzung hängen mit der besonderen berufsrechtlichen Stellung zusammen: Die Anwaltschaft verarbeitet zu einem ganz geringen Prozentsatz „eigene" Daten. Nahezu alles, was an Daten im Zuge der anwaltlichen Berufsausübung verarbeitet wird, sind Daten, die von Mandanten übergeben werden oder im Zuge von Verfahrensführung gewonnen werden. Diese Daten unterliegen der rechtsanwaltlichen Verschwiegenheitsverpflichtung. Diese ist kein Privileg der Rechtsanwälte, sondern vielmehr ein Recht der Mandanten und anderer betroffener Personen, welches von den Anwälten besonders sorgfältig geschützt wird. Diese der Verschwiegenheitsverpflichtung unterliegenden Daten genießen besonderen gesetzlichen Schutz und sind etwa auch nicht im Rahmen von Hausdurchsuchungen sicherstellbar. Eine „handelsübliche" Cloud zu verwenden, bei der Daten physisch außerhalb Österreichs gelagert werden und somit die nationalen Garantien für ihren Schutz nicht gegeben sind, ist daher rechtlich unzulässig.

Achtung, Vorgaben der DSGVO

Das bedeutet nicht zwingend, dass es keine Möglichkeit für den Einsatz einer „Anwaltscloud" gibt. Allerdings braucht es dafür wichtige Voraussetzungen: Die physische Datenhaltung muss in einer Jurisdiktion vorgenommen werden, welche dieselben oder bessere Standards für den Schutz der anwaltlichen Verschwiegenheit als Österreich aufweist. Und: Die Wege der Daten in und aus der Cloud dürften ebenso nur über derart geschützte Verbindungen laufen. Zudem muss sichergestellt werden, dass die Vorgaben der DSGVO eingehalten werden können, insbesondere betreffend den technischen Datenschutz und die Verständigungspflichten nach einem Datenverlust.

Sollten diese grundsätzlichen Vorgaben erfüllt werden und – verglichen mit dem Schutzniveau des Kanzleiservers – Daten mindestens gleich gut oder besser in der Cloud geschützt sein, wird auch die Angst der Anwaltschaft vor der Cloud der Vergangenheit angehören.


© Sergey Tarasov - stock.adobe.com

Cloud Computing klar geregelt

Der Rat der Anwaltschaften (Council of Bars and Law Societies in Europe, CCBE) hat zur Auswahl einer Cloud-Lösung und des IT-Dienstleisters Richtlinien für Rechtsanwälte aufgestellt. Darin ist geregelt: Der Datenspeicherort sollte im eigenen Land sein, was Cloud-Lösungen von Anbietern mit internationalen Rechenzentren ausschließt. Grundlagen müssen das jeweils anzuwendende Standesrecht, die Verschwiegenheitsverpflichtungen sowie die Datenschutzbestimmungen sein. In Österreich gilt konkret § 9 RAO, der aktuelle RL-BA sowie das Handbuch zur IT-Sicherheit in Rechtsanwaltskanzleien. Sofern die Grundlagen eine Verwendung der Cloud nicht verbieten, sind folgende Kriterien bei der Auswahl zu beachten:

- Klären Sie, ob ein Software as a Service (SaaS) oder ein Infrastructure as a Service (IAAS) Model verwendet wird und ob der Anbieter privat ist (Zusammenschluss von mehreren Privaten zur Schaffung einer gemeinsamen Cloud) oder öffentlich (jedem Marktteilnehmer eine Cloud-Lösung anbietend). Dies ist besonders für die Erfahrung, Spezialisierung, den Ruf und den Ort der Datenaufbewahrung von Bedeutung, wie auch für allfällige Interessenskonflikte, die Zahlungsfähigkeit des Cloud-Betreibers und Bestandsfähigkeit.
- Da Rechtsanwälte aufgrund ihrer Berufs- und Treuepflichten zur Herausgabe der Daten verpflichtet werden können, müssen Sie geeignete Maßnahmen treffen für den Fall der Insolvenz des Cloud-Providers, der Anwaltskanzlei oder eines Rechtsstreites, um die Daten zurückzuerhalten. Eventuell nicht nur vertraglich vorsorgen, sondern auch eine treuhänderische Verwaltung der Daten im Insolvenzfall regeln.
- Zum Thema Sicherheit verweist die CCBE (allerdings nicht abschließend) auf die herkömmlichen IT Risiko Management Standards für Sicherheitsmanagement ISO 27001:2005 und ISO 9001 für Qualitätsmanagement. Ein Passwortmanagement und Training für die Mitarbeiterinnen und Mitarbeiter der Kanzlei ist essentiell.
- Der Vertrag mit einem Cloud-Provider hat unter anderem Folgendes zu regeln: Verfügbarkeit, Service, Fehlerbehebung, Sub-Unternehmerregelung, Software-Lizenzen, technische Dokumentation, qualifizierte Vertraulichkeitsvereinbarung, treuhänderische Datenverwaltung im Fall der Insolvenz, Kündigungs- und Ausstiegsbestimmungen. Sollte der Standardvertrag des Providers hier nicht ausreichend sein, so ist darauf zu achten, dass dieser ergänzt wird.

Text: Sophie Martinetz