Foto: tostphoto – stock.adobe.com

Datenschutz im Cloud-Computing

Erklärungen zur IT-Sicherheitsrichtlinie der KZBV – Teil 4

In der Anlage 1 zur IT-Sicherheitsrichtlinie der KZBV wird empfohlen, im Zusammenhang mit der Verarbeitung personenbezogener Daten auf die Nutzung der in Office-Produkten integrierten Cloud-Speicherung zu verzichten (Kennung A1–05). Darüber hinaus häuft sich der Begriff „Cloud“ im Kapitel 9.4 des Leitfadens. Das Kapitel befasst sich mit dem Thema Datensicherung. Die Beschränkung auf Office-Integrationen und Datensicherung wird allerdings bei Weitem nicht der Bedeutung gerecht, die dem Cloud-Computing mittlerweile aufgrund seiner Verbreitung zukommt.

Verbreitet hat sich das Cloud-Computing, weil es einfach und komfortabel ist, sich Daten über mehrere Geräte synchronisieren lassen und viele Nutzer bislang dachten oder immer noch denken, die Daten in einer Cloud wären sicher. Zahlreiche Vorfälle der letzten Jahre, die ihren vorläufigen Höhepunkt im Brand gleich mehrerer Serverhallen eines französischen Rechenzentrumsbetreibers im Jahr 2021 fanden, haben aber gezeigt, dass ein allzu großes Vertrauen in Cloud-Computing schnell in einer Katastrophe enden kann. Warnungen werden vor dem Hintergrund vermeintlicher Vorteile des Cloud-Computings seit Jahren häufig ausgeblendet oder ignoriert.

Foto: Hans Schenkel

Dr. Thomas H. Lenhard ist ein international anerkannter Experte für Informationstechnologie und Datenschutz. Er greift auf seinen umfangreichen Erfahrungsschatz aus drei Jahrzehnten Datenschutz und Datensicherheit zurück und ist u.a. als Datenschutzbeauftragter sowohl für die DGZMK als auch für die DGI umfassend tätig.

Die Entscheidung, private Daten in einer öffentlichen Cloud abzulegen und die entsprechenden Risiken zu tragen, ist eine Sache. Geht es aber um Praxis- oder Gesundheitsdaten, sollte jedem klar sein, dass ein „Unfall“ mit Daten, die in einer Zahnarztpraxis verarbeitet werden, durchaus eine existenzielle Bedrohung darstellen kann.

Geht es um die Frage, ob man eine Cloud-Lösung verwenden kann, gilt es, zweierlei Aspekte zu klären. Erstens gilt es zu klären, um welche Cloud-Lösung es sich handelt. Zweitens spielt es eine wesentliche Rolle, welche Daten in dieser Cloud gespeichert werden sollen.

Die Frage nach der Art einer Cloud ist keinesfalls trivial, da der Begriff geradezu inflationär gebraucht wird und mitunter auch gewöhnliche Server, Online-Archive

oder Datenspeichergeräte als „Cloud“ bezeichnet werden. Welche Arten von Clouds gibt es also?

Grundsätzlich wird zunächst unterschieden zwischen einer privaten und einer öffentlichen Cloud. Bei der privaten Cloud werden innerhalb eines geschlossenen Systems ausschließlich Daten von den Verantwortlichen gespeichert oder verarbeitet.

Unternehmen oder auch medizinische Einrichtungen und Praxen können demnach eine Cloud auch ohne die Dienste eines entsprechenden Anbieters betreiben, selbst administrieren und den Betrieb auch auf eigenen Servern und im eigenen Serverraum realisieren.

Soweit ein solches System ausreichend abgesichert und sichergestellt ist, dass nur berechtigte Personen Zugriff auf die gespeicherten Daten erhalten, spricht aus Sicht des Datenschützers nichts dagegen, eine solche Lösung einzusetzen. Teilweise werden auch, wie bereits erwähnt, Archivsysteme als Cloud bezeichnet. Dies verdeutlicht, dass ein allgemeines „Cloud-Bashing“ nicht gerechtfertigt ist. Insbesondere, da hier durchaus sehr robuste und zuverlässige Systeme existieren.

Anders verhält es sich mit öffentlichen Clouds. Hier haben die Nutzer in der Regel keine Kontrolle darüber, auf welchen Servern, in welchen Rechenzentren oder gar in welchem Teil der Welt ihre Daten verarbeitet werden. Entgegen den sehr knappen Ausführungen im bereits erwähnten Leitfaden, besteht übrigens keinerlei Zweifel daran, dass die Nutzung einer öffentlichen Cloud durch ein Unternehmen oder eine Praxis zur Speicherung oder Verarbeitung personenbezogener Daten grundsätzlich eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO darstellt.

Insbesondere ein US-amerikanischer Anbieter öffentlicher Cloud-Systeme stellt diese Tatsache regelmäßig in Abrede. Um diesbezüglich Klarheit zu schaffen, haben die Datenschutzbeauftragten aus Bund und Ländern (Datenschutzkonferenz, kurz: DSK) eine Orientierungshilfe zum Thema Cloud-Computing veröffentlicht. In dieser wird klargestellt, dass – erstens – eine Verschlüsselung von Daten eine technisch-organisatorische Maßnahme ist, die grundsätzlich erforderlich ist, wenn personenbezogene Daten in einer Cloud gespeichert werden. Zweitens wird betont, dass die Daten durch diese Verschlüsselung regelmäßig ihren Personenbezug nicht verlieren. Sowohl die DSK wie auch das Bayrische Landesamt für Datenaufsicht haben darüber hinaus Informationen veröffentlicht, wonach „*Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist*“, regelmäßig eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO darstellt.

Ein ‚Cloud-Bashing‘ ist nicht gerechtfertigt, da durchaus sehr robuste und zuverlässige Systeme existieren.

Kaum jemand wird Ihnen regelmäßig ähnlich dreiste Unwahrheiten auftischen wie Vertriebsleute, die Sie von der Sicherheit und Zulässigkeit einer außereuropäischen Cloud-Lösung überzeugen möchten. Unter den Cloud-Anbietern gibt es sogar ein Unternehmen, dass sich regelmäßig weigert, Verträge über eine Auftragsverarbeitung abzuschließen, von der EU vorgegebene Standardvertragsklauseln ignoriert und auch sonst keine sonderliche Bereitschaft zeigt, geltende Vorschriften zum Datenschutz in der EU einzuhalten.

Durch das Urteil „Schrems II“ des EuGH ist derzeit eine Übermittlung von personenbezogenen Daten in die USA generell schon schwierig. Darüber hinaus nehmen die USA für sich in Anspruch, auch auf Daten europäischer Bürger außerhalb der USA zugreifen zu können, was einen klaren Verstoß gegen europäisches Recht darstellen dürfte.

Die einschlägigen Empfehlungen der KZBV sind daher, in Anbetracht der derzeitigen Lage, nur allzu gut nachvollziehbar. Eine Änderung der Situation im Zusammenhang mit den USA wäre zwar dringend erforderlich, ist jedoch derzeit nicht absehbar.

Daten gelten bereits als in ein Drittland übermittelt, wenn aus diesem Land ein administrativer Zugriff auf Systeme in der EU erfolgt. Wenn nun also die Daten als übermittelt gelten und darüber hinaus die USA sich das Recht vorbehalten, auch auf Daten zuzugreifen, die in Europa gespeichert werden, kann die Situation nicht dadurch verbessert werden, dass US-Unternehmen darauf verweisen, dass möglicherweise die Daten der Nutzer nur in Rechenzentren in Europa gespeichert würden.

Glücklicherweise gibt es auch noch Anbieter von Cloud-Lösungen, die ihren Sitz in Europa oder in einem Land haben, für das ein Angemessenheitsbeschluss der EU besteht und wo generell von einem angemessenen Datenschutzniveau ausgegangen werden kann.

Hier ist aber gleichwohl ebenfalls Vorsicht geboten. Immer wieder wird mit deutschen oder europäischen Lösungen geworben – wohl wissend, dass eine Übermittlung von personenbezogenen Daten in die USA mitunter derzeit höchst illegal sein könnte. Bei einigen Anbietern solcher „europäischer Lösungen“ zeigt sich, dass zwar die Bedieneroberfläche einer internetbasierten Software möglicherweise durch ein deutsches oder europäisches Unternehmen erstellt worden ist, jedoch vollständig auf der Technik eines US-Unternehmens aufbaut und darüber hinaus die Nutzerdaten in einer Cloud-Lösung dieses US-Anbieters gespeichert werden.

Einige Anbieter webbasierter Lösungen haben offensichtlich keinerlei Skrupel, ihre Kunden dreist hinters Licht zu führen. Einige Unternehmen weigern sich z.B. auch Verträge nach Art. 28 DSGVO zu schließen oder verweigern jede Auskunft über den Ort der Datenspeicherung. Wenn diese Firmen sich dabei dann auch noch auf die DSGVO berufen, schlägt das eigentlich dem Fass den Boden aus. Derartige Verhaltensweisen dürften bereits ein deutliches Indiz dafür sein, dass im Geschäftsbetrieb eines solchen Unternehmens datenschutzrechtliche Vorschriften keinen sonderlich hohen Stellenwert einnehmen.

Die Nutzung einer Cloud-Lösung befreit übrigens nicht davon, ein valides Da-

tensicherungskonzept vorzuhalten (siehe Beitrag in der ZZI Ausgabe 1/2021). Was die Nutzung einer Cloud-Lösung zum Zweck der zusätzlichen Datensicherung betrifft, gelten die gleichen Voraussetzungen wie für die sonstige Nutzung. Schließlich finden sich in der Datensicherung die gleichen Daten wie in den Systemen, die gesichert wurden. Das bedeutet: Wenn wir unsere Echtdaten nicht in ein bestimmtes Cloud-System übertragen dürfen, darf dort auch keine Sicherung der entsprechenden Daten abgelegt werden. Allerdings ist eine redundante Sicherung grundsätzlich sinnvoll.

Natürlich gibt es auch zahlreiche seriöse Anbieter von Cloud-Systemen am Markt. Die Frage ist aber, ob man wirklich solche Lösungen braucht. Ein öffentliches Cloud-System, in dem Milliarden von Datensätzen aus allen denkbaren Unternehmen und Organisationen gespeichert werden, weckt bei Hackern nicht nur besondere Begehrlichkeiten, es wird auch eher mittels gezielter Maßnahmen angegriffen als eine private Cloud, die nur per VPN oder über interne Netze erreichbar ist.

Fazit: Der Einsatz eines privaten Cloud-Systems kann durchaus in einer Zahnarztpraxis oder in einem MVZ erfolgen, wenn grundlegende Erfordernisse des Datenschutzes beachtet werden. Hinsichtlich der Nutzung öffentlicher Cloud-Systeme ist die Empfehlung des KZBV nachvollziehbar. Cloud-Computing beschränkt sich allerdings nicht auf die bloße Speicherung von Dateien. Beim Einsatz von webbasierten Softwarelösungen ist ebenso Vorsicht geboten.

Wenn ein Anbieter eines webbasierten Systems, in dem personenbezogene Daten verarbeitet werden, nicht in der Lage oder nicht willens ist, Ihnen einen Standardvertrag nach Art. 28 DSGVO zukommen zu lassen, obwohl der Anbieter das System technisch betreut und sich eventuelle sogar per Fernwartung auf Systeme Ihrer Praxis einwählt, so sollten Sie vom Einsatz eines entsprechenden Anbieters eher Abstand nehmen. Das gilt übrigens auch für Software, die in der Praxis installiert und von einem Dienstleister betreut wird. Die Fernwartung von Systemen ist ebenfalls eine Auftragsverarbeitung und die Durchführung der Tätigkeiten ohne eine Vereinbarung nach Art. 28 DSGVO ist nicht zulässig.

Wie sich in der Praxis zeigt, kann die Nutzung einer Cloud-Lösung selbst bei Konstellationen mit mehreren Standorten in aller Regel vermieden werden, in dem z.B. mit einem geeigneten Archivsystem gearbeitet wird. Denken Sie immer daran: Trotz aller Versprechen von Vertriebsprofis von Cloud-, Portal- und Softwareanbietern sind immer nur Sie verantwortlich für die Daten Ihrer Mitarbeiter und Ihrer Patienten.

Hilfe bei Fragen: Schreiben Sie eine Mail an: dr.lenhard@it-planung.com mit dem Betreff „Artikel in der ZZI 02/2022“

→ **Dr. Thomas H. Lenhard**

CHECKLISTE CLOUD

1. Trifft es zu, dass Sie keine Cloud-basierte Office-Lösung nutzen?

2. Falls Sie eine private Cloud nutzen:
   a. Läuft die private Cloud auf eigener Hardware?
   b. Ist die private Cloud nur intern oder über eine sichere VPN-Verbindung erreichbar?
   c. Ist eine Verbindung direkt per Remote Desktop (RDP) über das Internet nicht möglich, ohne zuvor eine VPN-Verbindung aufzubauen?
   d. Für die VPN-Verbindung wird eine Verschlüsselung eingesetzt, die dem Stand der Technik entspricht (z.B. AES-256)?
   e. Wurde die Firewall, über die die VPN-Verbindung aufgebaut wird, in den letzten drei Monaten mindestens einmal aktualisiert (Update)?

3. Falls Sie eine öffentliche Cloud nutzen:
   a. Ist sichergestellt, dass keine besonders schützenswerten Daten in der Cloud gespeichert werden?
   b. Existiert ein Vertragswerk nach Art. 28 DSGVO?
   c. Ist sichergestellt, dass keine personenbezogenen Daten in ein unsicheres Drittland (z.B. USA) übermittelt werden?
   d. Sind die Daten, welche Sie in der Cloud speichern verschlüsselt?

4. Falls Sie eine internetbasierte Applikation einsetzen:
   a. Ist ein Vertrag nach Art. 28 DSGVO mit dem Anbieter geschlossen worden?
   b. Kennen Sie den Ort der Speicherung der im System verarbeiteten personenbezogenen Daten?
   c. Ist sichergestellt, dass die Datenspeicherung nur innerhalb des EWR erfolgt oder zumindest in einem Drittland, für das ein Angemessenheitsbeschluss der EU besteht?
   d. Ist sichergestellt, dass der Anbieter keine Daten in einer Cloud anderer Anbieter speichert?
   e. Sind Ihnen alle Unterauftragnehmer des Anbieters bekannt?

Soweit Sie eine oder mehrere Fragen mit Nein beantwortet haben, besteht hinsichtlich der Cloud-Nutzung Verbesserungspotenzial.